УТВЕРЖДАЮ

Директор ФГУП «РНИИРС»

[redacted]

«___» __________ 2017 г.

УТВЕРЖДАЮ

Генеральный директор
ООО «НТЦ «Вулкан»

А.В. Марков

«___» __________ 2017 г.

ПРОГРАММА И МЕТОДИКИ ПРЕДВАРИТЕЛЬНЫХ ИСПЫТАНИЙ

опытного образца «Амезит-В»

(Шифр «Амезит-В»)

ВАТС.466535.135ПМ

Листов 333

СОГЛАСОВАНО

Начальник 474 ВП МО РФ

[redacted]

«___» __________ 2017 г.

2017

СОДЕРЖАНИЕ

1 Программа испытаний

1.1Объект испытаний

1.1.1 Объектом предварительных испытаний является опытный образец (далее – ОО) специального программного обеспечения (СПО) «Амезит-В» RU.ВАТС.00176-01 (далее – СПО «Амезит), изготовленный ООО «НТЦ «Вулкан», являющееся составной частью аппаратно-программного комплекса (АПК) «Амезит».

1.2Цель и задачи испытаний

1.2.1 Предварительные испытания опытного образца СПО «Амезит-В» проводят с целью проверки соответствия его требованиям технического задания (ТЗ) на СЧ ОКР «Амезит-В» и Дополнения № 1 к нему, а также определения готовности опытного образца СПО «Амезит-В» к межведомственным испытаниям.

1.2.2 Задачами испытаний являются:

- проверка комплектности опытного образца;
- проверка на соответствие к основным параметрам и характеристикам опытного образца;
- предварительной оценка достаточности и полноты документации;
- определения возможности предъявления опытного образца и разработанной РКД на межведомственные испытания.

1.3Общие положения

1.3.1 Предварительные испытания проводяться на основании следующих документов:

- Договор № 1/16.16 от 30.09.2016 г.;
- ТЗ на составную часть опытно-конструкторской работы (далее – ТЗ на СЧ ОКР) «Амезит-В» (Приложение № 1 к договору № 1/16.16 от 30.09.2016 г.);
- Дополнение № 1 к техническому заданию на составную часть опытно-конструкторской работы;
- уведомление о готовности Исполнителя к проведению предварительных испытаний опытного образца СПО «Амезит-В»;
- приказ директора ООО «НТЦ «Вулкан» о назначении комиссии ро проведению предварительных испытаний опытного образца СПО «Амезит-В»;
- «Программа и методики предварительных испытаний»;
- комплект конструкторской и программной документации.

1.3.2 На предварительные испытания предъявляют опытный образец СПО «Амезит-В», проверенный и принятый ОТК ООО «НТЦ «Вулкан» и 474

ВП МО РФ в объеме проверок, соответствующих категории приемосдаточных испытаний.

1.3.3 Испытания проводятся по «Программе и методикам предварительных испытаний…» (далее – ПМ), разработанной ООО «НТЦ «Вулкан», согласованной и утвержденной установленным порядком в соответствии с ГОСТ РВ 15.211-2002.

1.3.4 О готовности к проведению предварительных испытаний ООО «НТЦ «Вулкан» извещает Заказчика уведомлением, согласованным с 474 ВП МО РФ.

1.3.5 Сроки проведения предварительных испытаний определяются приказом директора ООО «НТЦ «Вулкан» в местах размещения опытного образца.

1.3.6 Для проведения предварительных испытаний создается комиссия, в состав которой включаются представители ООО «НТЦ «Вулкан», ФГУП «РНИИРС» и 474 ВП МО РФ (по согласованию).

1.3.7 В своей работе комиссия руководствуется требованиями ГОСТ РВ 15.210-2001 (в части порядка проведения предварительных испытаний) и нормативно-техническими документами, приведенными в приложении А.

1.3.8 Результаты испытаний фиксируются в протоколах. В процессе испытаний комиссия имеет право совмещать во времени испытания по нескольким пунктам настоящей программы с отражением результатов испытаний в едином протоколе. Допускается уточнять методики испытаний, если эти уточнения не снижают их достоверность по сравнению с методиками, настоящей программы.

1.3.9 Комиссия по проведению предварительных испытаний может приостановить или прекратить испытания. Основанием для принятия такого решения могут быть:

- несоответствие опытного образца СПО «Амезит-В» требованиям ТЗ на СЧ ОКР «Амезит-В» или требованиям программной документации;
- отказ испытываемого опытного образца АПК «Амезит», препятствующий дальнейшему проведению испытаний.

1.3.10 Решение о приостановке (перерыве) испытаний принимает комиссия, проводящая испытания. Приостановка испытаний оформляется протоколом комиссии. В протоколе устанавливается продолжительность перерыва испытаний и, при необходимости, объем работ по повторным проверкам опытного образца после устранения причин приостановки.

1.3.11 Прекращение испытаний оформляют актом, который должен быть подписан всеми членами комиссии и направлен для принятия соответствующего решения Заказчику и исполнителю СЧ ОКР «Амезит-В».

1.3.12 Перед возобновлением испытаний, комиссия проверяет материалы, в которых отражены результаты устранения причин прекращения (перерыва) испытаний, проверки полноты доработок опытного образца, осуществленных по предложениям комиссии, прекратившей испытания.

1.3.13 Испытания считают законченными, если их результаты оформлены актом, подтверждающим выполнение программы испытаний и содержащим оценку результатов испытаний.

1.3.14 Комиссии разрешается при необходимости корректировать программу и методики испытаний.

1.4Объем испытаний

1.4.1 Изделие подлежит испытаниям в объеме, указанном в таблице 1.

Таблица 1 – Объем испытаний

№ п/п	Наименование испытаний и проверок	Номер		Примечание
		пункта ТЗ, Дополнения №1 к ТЗ	методики испытаний	
1	Проверка достаточности и полноты документации СПО «Амезит-В»	5.1.1–5.1.4, 9.5, 13.2.5–13.2.6, 13.3, 13.5.1–13.5.8, 13.6.1, 13.11–13.13, 13.17–13.19	Методика № 1	
2	Проверка комплектности СПО «Амезит-В»	3.1, 5.4.2.2, 5.4.2.3, 9.14, 13.14	Методика № 2	
3	Проверка выполнения требований назначения СПО формирования автономного сегмента сети передачи данных (СПО ПАС)	3.2.1		
3.1	Проверка ретрансляции трафика и организации подключения к проводным линиям связи	3.2.1.1	Методика № 3	
3.2	Проверка ретрансляции трафика с использованием	3.2.1.2	Методика № 4	

№ п/п	Наименование испытаний и проверок	Номер		Примечание
		пункта ТЗ, Дополнения №1 к ТЗ	методики испытаний	
	беспроводных линий и организации подключения к беспроводным сетям связи			
3.3	Проверка управления сторонним телекоммуникационным оборудованием уровня распределения и уровня ядра без авторизации и при наличии к нему физического доступа	3.2.1.3	Методика № 5	
3.4	Проверка сбора, регистрации и отображения информации	3.2.1.4	Методика № 6	
3.5	Проверка маршрутизации трафика и передачи его на технические средства первичного анализа информации	3.2.1.5	Методика № 7	
3.6	Проверка автоматической настройки сети с использованием протоколов DHCP, NTP, DNS	3.2.1.6	Методика № 8	
3.7	Проверка приоритизации трафика с использованием TOS	3.2.1.7	Методика № 9	
3.8	Проверка балансировки нагрузки с динамическим распределением ресурсов	3.2.1.8	Методика № 10	
3.9	Проверка автоматизированного управления модулями ретрансляции с предоставлением единого графического интерфейса	3.2.1.9	Методика № 11	
3.10	Проверка сетевой трансляции адресов	3.2.1.10	Методика № 12	
3.11	Проверка возможности устойчивого к несанкционированному доступу централизованного управления и мониторинга	3.2.1.11	Методика № 13	

№ п/п	Наименование испытаний и проверок	Номер		Примечание
		пункта ТЗ, Дополнения №1 к ТЗ	методики испытаний	
	контролируемого оборудования с использованием единого графического интерфейса			
3.12	Проверка сопряжения с каналообразующей аппаратурой различных опорных сетей передачи данных	3.2.1.12	Методика № 14	
3.13	Проверка скорости передачи данных	3.2.1.13	Методика № 15	
3.14	Проверка контроля состояния телекоммуникационного оборудования, оперативного выявления попыток получения НСД к ним, нештатных перезагрузок ОС аппаратного обеспечения и иных фактов нарушения ИБ подсистемы ПАС	3.2.1.14	Методика № 16	
4	Проверка выполнения требований назначения СПО контроля сообщений автономного сегмента сети передачи данных (СПО ПКС)	3.2.2		
4.1	Проверка анализа соединений автономного сегмента сети передачи данных и сбора информации на скорости до 6 Гбит/с	3.2.2.1	Методика № 17	
4.2	Проверка организации узлов промежуточного контроля с целью анализа соединений и выявления информации при использовании протоколов типа IPSEC	3.2.2.2	Методика № 18	
4.3	Проверка автоматического распознавания и отбора файлов	3.2.2.3	Методика № 19	
4.4	Проверка предотвращения использования технологий	3.2.2.4	Методика № 20	

№ п/п	Наименование испытаний и проверок	Номер		Примечание
		пункта ТЗ, Дополнения №1 к ТЗ	методики испытаний	
	анонимизации пользователей			
4.5	Проверка блокировки и перенаправления клиентских запросов (HTTP/HTTPS) на легитимные ресурсы ГИС ОП (зеркала)	3.2.2.5	Методика № 21	
4.6	Проверка возможности выбора заданного абонента	3.2.2.6	Методика № 22	
4.7	Проверка формирования, отображения и экспорта списков абонентов-отправителей и абонентов-получателей с топологическими связями между ними	3.2.2.7	Методика № 23	
4.8	Проверка ведения статистики сетевой активности	3.2.2.8	Методика № 24	
4.9	Проверка регистрации в накопитель информационного обмена (в полном объеме) для абонента, задаваемого оператором	3.2.2.9	Методика № 25	
4.10	Проверка визуализации трафика и анализа связей участников соединений до требуемого уровня	3.2.2.10	Методика № 26	
4.11	Проверка осуществления распределенных вычислений в целях поиска ключевой информации	3.2.2.11	Методика № 27	
5	Проверка выполнения требований назначения СПО мониторинга сети Интернет и СМИ (СПО ПМС)	3.2.3		
5.1	Проверка сбора информации из социальных сетей, блогов, микроблогов, форумов, а также новостных информационных порталов в заданном	3.2.3.1	Методика № 28	

№ п/п	Наименование испытаний и проверок	Номер		Примечание
		пункта ТЗ, Дополнения №1 к ТЗ	методики испытаний	
	географическом регионе			
5.2	Проверка выявления источника появления информации	3.2.3.2	Методика № 29	
5.3	Проверка анализа распространения информации с представлением результатов в графическом виде (в виде графа распространения)	3.2.3.3	Методика № 30	
5.4	Проверка анализа эмоциональной окраски информационных материалов	3.2.3.4	Методика № 31	
5.5	Проверка непрерывного целевого поиска и отбора разнородной информации в цифровых источниках открытого доступа по заданной тематической направленности с осуществлением географической идентификации, ее совместного комплексного анализа на геопространственной основе	3.2.3.5	Методика № 32	
5.6	Проверка визуализации обобщенных результатов тематического отбора информации из открытых цифровых источников на цифровой интерактивной модели земного шара (ГИС) с возможностью детализации интересующих материалов и их отбора	3.2.3.6	Методика № 33	
5.7	Проверка формирования шаблонов обработки цифровых источников открытого доступа с указанием регионов, информацию в которых необходимо собирать	3.2.3.7	Методика № 34	

№ п/п	Наименование испытаний и проверок	Номер		Примечание
		пункта ТЗ, Дополнения №1 к ТЗ	методики испытаний	
5.8	Проверка поиска, выявления на основе ключевых признаков и представления на анализ оператору новых информационных ресурсов для определения необходимости сбора информации	3.2.3.8	Методика № 35	
5.9	Проверка автоматизированного составления аналитических справок о различных событиях, объектах и персонах в заданном интервале времени по временным, адресным, региональным параметрам и по источникам их появления	3.2.3.9	Методика № 36	
5.10	Проверка того, что действия СПО ПМС не определяются как элементы инфраструктуры государственных органов	3.2.3.10	Методика № 37	
5.11	Проверка возможности автоматизированного взаимодействия с СПО подсистемы лингвистического обеспечения	3.2.3.11	Методика № 38	
5.12	Проверка возможности удаленного использования СПО ПМС территориально распределенными элементами АПК «Амезит» (через подсистему ППД) с разграничением прав доступа согласно ролевой модели доступа	3.2.3.12	Методика № 39	
6	Проверка выполнения требований назначения СПО контроля информационно-технических объектов телекоммуникационных систем и систем жизнеобеспечения	3.2.4		

№ п/п	Наименование испытаний и проверок	Номер		Примечание
		пункта ТЗ, Дополнения №1 к ТЗ	методики испытаний	
	(СПО ПОТ)			
6.1	Проверка тестирования телекоммуникационного оборудования уровня распределения и уровня ядра на возможность проникновения внешнего нарушителя и возможность установки сторонних модулей расширения	3.2.4.1	Методика № 40	
6.2	Проверка проведения нагрузочного и функционального тестирования, направленных на блокирование работы телекоммуникационного оборудования	3.2.4.2	Методика № 41	
6.3	Проверка создания и изготовления стенда контроля информационно-технических объектов систем жизнеобеспечения с возможностью визуализации механизмов проведения воздействий	3.2.4.3	Методика № 42	
6.4	Проверка разработки сборника методик реверс-инжиниринга встроенного ПО (ВПО)	3.2.4.4	Методика № 43	
7	Проверка выполнения требований назначения СПО первичного анализа информации (СПО ППА)	3.2.5		
7.1	Проверка анализа соединений технических средств автономного сегмента сети передачи данных и сбора информации	3.2.5.1	Методика № 44	
7.2	Проверка организации узлов промежуточного контроля с целью получения доступа к	3.2.5.2	Методика № 45	

№ п/п	Наименование испытаний и проверок	Номер		Примечание
		пункта ТЗ, Дополнения №1 к ТЗ	методики испытаний	
	информации, передаваемой с использованием протоколов типа IPSEC			
7.3	Проверка автоматического распознавания и отбора файлов	3.2.5.3	Методика № 46	
7.4	Проверка автоматизированной подготовки и развертывания в автономном сегменте сети передачи данных «двойников» для легитимных ресурсов ГИС ОП	3.2.5.4	Методика № 47	
7.5	Проверка блокировки и перенаправления клиентских запросов (HTTP/HTTPS) на легитимные ресурсы ГИС ОП (зеркала)	3.2.5.5	Методика № 48	
7.6	Проверка возможности выбора заданного абонента автономного сегмента сети передачи данных путем задания оператором совокупности коммутационно-адресных признаков, в том числе IP-адреса, IP-маски, MAC-адреса, адреса для протоколов прикладного уровня	3.2.5.6	Методика № 49	
7.7	Проверка выявления каналов передачи данных систем связи и управления противодействующей стороны	3.2.5.7	Методика № 50	
7.8	Проверка нарушения штатного функционирования коммуникационного оборудования с использованием технических средств контроля объектов телекоммуникационных систем	3.2.5.8	Методика № 51	
7.9	Проверка определения режима	3.2.5.9	Методика	

№ п/п	Наименование испытаний и проверок	Номер		Примечание
		пункта ТЗ, Дополнения №1 к ТЗ	методики испытаний	
	работы и состава телекоммуникационного оборудования		№ 52	
7.10	Проверка выявления каналов передачи данных критически важных информационных объектов	3.2.5.10	Методика № 53	
7.11	Проверка выявления информационных ресурсов противодействующей стороны	3.2.5.11	Методика № 54	
7.12	Проверка регистрации в накопитель информационного обмена (в полном объеме) абонента, задаваемого оператором	3.2.5.12	Методика № 55	
7.13	Проверка обеспечения программными средствами первичного анализа информации выполнения требований назначения	3.2.5.13	Методика № 56	
7.14	Проверка сопряжения с каналообразующей аппаратурой различных опорных сетей передачи данных	3.2.5.14	Методика № 57	
8	Проверка выполнения требований назначения СПО ретрансляции данных с использованием промежуточных серверов (СПО ПРД)	3.2.6		
8.1	Проверка выполнения функций ретрансляции данных в целях реализации скрытого обмена между техническими средствами мониторинга сети Интернет и ресурсами ГИС Интернет по протоколам семейства TCP/IP	3.2.6.1	Методика № 58	

№ п/п	Наименование испытаний и проверок	Номер		Примечание
		пункта ТЗ, Дополнения №1 к ТЗ	методики испытаний	
8.2	Проверка выполнения функций ретрансляции данных в целях реализации скрытого обмена между техническими средствами подготовки, размещения и «раскрутки» специальных материалов и ресурсами ГИС Интернет по протоколам семейства TCP/IP	3.2.6.2	Методика № 59	
8.3	Проверка построения рациональных с точки зрения скрытности и скорости обмена информацией виртуальных транспортных маршрутов ретрансляции данных	3.2.6.3	Методика № 60	
8.4	Проверка подключения автоматизированных рабочих мест операторов АПК «Амезит» к системе обмена данными, не требующего дополнительных настроек для пользователей	3.2.6.4	Методика № 61	
8.5	Проверка автоматического построения виртуальных маршрутов	3.2.6.5	Методика № 62	
8.6	Проверка сокрытия персонализирующей информации о средствах передачи данных от средств мониторинга и анализа противодействующей стороны	3.2.6.6	Методика № 63	
8.7	Проверка сокрытия информации о национальной принадлежности	3.2.6.7	Методика № 64	
8.8	Проверка маскирования данных на узлах ретрансляции под легальные пользовательские запросы к общедоступным сервисам	3.2.6.8	Методика № 65	

№ п/п	Наименование испытаний и проверок	Номер		Примечание
		пункта ТЗ, Дополнения №1 к ТЗ	методики испытаний	
8.9	Сокрытие персонализирующей информации прикладного уровня должно контролироваться СПО, устанавливаемым на АРМ оператора	3.2.6.9	Методика № 66	
8.10	Проверка создания виртуальных маршрутов по настраиваемым администратором шаблонам	3.2.6.10	Методика № 67	
8.11	Проверка возможности централизованного управления СПО ретрансляции данных (в ручном и автоматизированном режиме)	3.2.6.11	Методика № 68	
8.12	Проверка возможности прогноза скорости передачи данных с использованием виртуального транспортного маршрута	3.2.6.12	Методика № 69	
8.13	Проверка контроля работоспособности точек виртуальных маршрутов	3.2.6.13	Методика № 70	
8.14	Проверка выполнения функций добавления шумовых конструкций в целях статистического камуфлирования данных, проходящих через технические средства ретрансляции данных, под легальные пользовательские запросы к общедоступным сервисам	3.2.6.14	Методика № 71	
8.15	Проверка сокрытия истинного назначения группировки точек виртуальных маршрутов	3.2.6.15	Методика № 72	
8.16	Выполнение требований СПО ретрансляции данных в части	3.2.6.16	Методика № 73	

№ п/п	Наименование испытаний и проверок	Номер		Примечание
		пункта ТЗ, Дополнения №1 к ТЗ	методики испытаний	
	СПО мониторинга сети Интернет и «раскрутки» материалов должно выполняться различными способами и не допускать раскрытия информации при вскрытии одного из них			
8.17	Проверка блокирования любых непосредственных взаимодействий технических средств раскрутки материалов и мониторинга сети Интернет в обход системы ретрансляции данных	3.2.6.17	Методика № 74	
8.18	Проверка предоставления шлюза анонимизации, обеспечивающего механизмы сопряжения для других технических средств АПК «Амезит» (в том числе территориально удаленных)	3.2.6.18	Методика № 75	
8.19	Проверка обнаружения и противодействия попыткам запуска специального программного обеспечения в виртуальной среде и под управлением отладчиков	3.2.6.19	Методика № 76	
8.20	Проверка обеспечения контроля состояния группировки точек виртуальных маршрутов, оперативного выявления попыток получения НСД к ним, нештатных перезагрузок ОС аппаратного обеспечения и иных фактов нарушения информационной безопасности (ИБ) технических средств ретрансляции	3.2.6.20	Методика № 77	
8.21	Проверка протоколирования	3.2.6.21	Методика	

№ п/п	Наименование испытаний и проверок	Номер		Примечание
		пункта ТЗ, Дополнения №1 к ТЗ	методики испытаний	
	действий технических средств ретрансляции данных на АРМ управления ретрансляции		№ 78	
8.22	В случае нештатных ситуаций, попыток анализа СПО ретрансляции данных, а также по команде администратора все модули СПО, конфигурационные файлы, входные и выходные данные СПО ретрансляции должны быть уничтожены	9.12	Методика № 79	
9	Проверка выполнения требований назначения СПО подготовки, размещения и «раскрутки» специальных материалов (СПО ПРР)	3.2.7		
9.1	Проверка подготовки специальных материалов (текстовых, графических, видео-, аудиосообщений)	3.2.7.1	Методика № 80	
9.2	Проверка обеспечения скрытия и генерации легендированной персонализирующей информации в специальных материалах очисткой или заполнением метаданных	3.2.7.2	Методика № 81	
9.3	Проверка обхода ограничений дополнительных параметров приватности в социальных сетях	3.2.7.3	Методика № 82	
9.4	Проверка автоматизированного размещения специальных материалов	3.2.7.4	Методика № 83	
9.5	Проверка обеспечения средств поднятия рейтингов распространяемых специальных материалов	3.2.7.5	Методика № 84	

№ п/п	Наименование испытаний и проверок	Номер		Примечание
		пункта ТЗ, Дополнения №1 к ТЗ	методики испытаний	
9.6	Проверка автоматизированной регистрации учетных записей пользователей с использованием генерируемых (с учетом технологий социальной инженерии) личных данных	3.2.7.6	Методика № 85	
9.7	Проверка создания копии профиля реально существующего субъекта	3.2.7.7	Методика № 86	
9.8	Проверка поддержки не менее 100 профилей пользователей социальных сетей с одного рабочего места	3.2.7.8	Методика № 87	
9.9	Проверка автоматизированной подготовки электронной почты (Yandex, Mail.ru, Gmail) при регистрации учетных записей в поддерживаемых сервисах	3.2.7.9	Методика № 88	
9.10	Проверка подготовки, хранения и представления оператору профиля виртуального пользователя: личные данные, имеющиеся учетные записи в поддерживаемых сервисах, история действий, личные диалоги в имеющихся учетных записях	3.2.7.10	Методика № 89	
9.11	Проверка анализа и генерации отчетов о внешней по отношению к профилю активности	3.2.7.11	Методика № 90	
9.12	Проверка распространения информационных сообщений абонентам ГИС ОП посредством электронной почты	3.2.7.12	Методика № 91	
9.13	Проверка распространения	3.2.7.13	Методика	

№ п/п	Наименование испытаний и проверок	Номер		Примечание
		пункта ТЗ, Дополнения №1 к ТЗ	методики испытаний	
	информационных сообщений абонентам ГИС ОП через автоматизированную рассылку личных сообщений в поддерживаемых сервисах		№ 92	
9.14	Проверка распространения информационных сообщений абонентам по телефонным сетям с использованием технологии IP-телефонии	3.2.7.14	Методика № 93	
9.15	Проверка распространения информационных сообщений абонентам посредством SMS-/MMS-сообщений	3.2.7.15	Методика № 94	
9.16	Проверка информационного обеспечения мероприятий по распространению специальных материалов в поддерживаемых сервисах	3.2.7.16	Методика № 95	
9.17	Проверка обеспечения «эффекта реального пользователя» в процессе распространения информационных материалов	3.2.7, 3.2.7.17	Методика № 96	
9.18	Проверка механизмов препятствия раскрытию национальной и ведомственной принадлежности	3.2.7.18	Методика № 97	
9.19	Проверка автоматизированного взаимодействия с СПО подсистемы лингвистического обеспечения	3.2.7.19	Методика № 98	
9.20	Проверка выполнения требований по режиму обработки данных и правам по доступу к обрабатываемой информации	9.3.2, 9.3.3	Методика № 99	
9.21	Проверка функций регистрации	9.17	Методика	

№ п/п	Наименование испытаний и проверок	Номер		Примечание
		пункта ТЗ, Дополнения №1 к ТЗ	методики испытаний	
	и хранения действий операторов		№ 100	
10	Проверка выполнения требований назначения СПО тестирования телекоммуникационного оборудования (СПО ПТТ)	3.2.8		
10.1	Проверка обнаружения актуальных критических уязвимостей системного ПО	3.2.8.1	Методика № 101	
10.2	Проверка обнаружения актуальных критических уязвимостей серверного ПО	3.2.8.2	Методика № 102	
10.3	Проверка обнаружения актуальных критических уязвимостей ПО защиты информации	3.2.8.4	Методика № 103	
10.4	Проверка структурного и статического анализа исходных текстов программ	3.2.8.5	Методика № 104	
10.5	Проверка динамического анализа программного обеспечения	3.2.8.6	Методика № 105	
10.6	Проверка автоматизированного распознавания используемых стандартных библиотечных функций	3.2.8.7	Методика № 106	
10.7	Проверка сигнатурного анализа потенциально опасных операций	3.2.8.8	Методика № 107	
10.8	Проверка восстановления логики функционирования и протоколов сетевого взаимодействия программного обеспечения сторонних разработчиков	3.2.8.9	Методика № 108	
10.9	Автоматизированная проверка СПО АПК «Амезит» САВЗ	3.2.8.10	Методика № 109	

№ п/п	Наименование испытаний и проверок	Номер		Примечание
		пункта ТЗ, Дополнения №1 к ТЗ	методики испытаний	
10.10	Проверка автоматизированного обновления баз вирусных сигнатур из доверенных источников	3.2.8.11	Методика № 110	
10.11	Проверка автоматизированного поиска внесенных изменений в программный код системного и прикладного ПО сторонних разработчиков при его модификации	3.2.8.12	Методика № 111	
10.12	Проверка моделирования угроз информационной безопасности	3.2.8.13	Методика № 112	
10.13	Проверка моделирования элементов и сегментов компьютерных сетей автономного сегмента для тестирования функциональных возможностей средств защиты информации	3.2.8.14	Методика № 113	
11	Проверка выполнения требований назначения СПО хранения данных (СПО ПХД)	3.2.9		
11.1	Проверка хранения информации, собранной с помощью подсистем ПМС и ПКС	3.2.9.1	Методика № 114	
11.2	Проверка хранения шаблонов обработки новостных информационных порталов	3.2.9.2	Методика № 115	
11.3	Проверка хранения аналитических справок, подготовленных в АПК «Амезит»	3.2.9.3	Методика № 116	
11.4	Проверка структурирования информации	3.2.9.4	Методика № 117	
11.5	Проверка поиска данных в массивах информации	3.2.9.5	Методика № 118	
11.6	Проверка предоставления	3.2.9.6	Методика	

№ п/п	Наименование испытаний и проверок	Номер		Примечание
		пункта ТЗ, Дополнения №1 к ТЗ	методики испытаний	
	оператору информации в графическом виде		№ 119	
11.7	Проверка резервного копирования данных	3.2.9.7	Методика № 120	
11.8	Проверка хранения видео-, аудиоархивов	3.2.9.8	Методика № 121	
11.9	Проверка одновременного просмотра архивов (до 3 подключений) без остановки записи	3.2.9, 3.2.9.9	Методика № 122	
11.10	Проверка автоматизированного взаимодействия с СПО подсистемы лингвистического обеспечения	3.2.9.14	Методика № 123	
12	Проверка выполнения требований назначения СПО обработки результатов и их визуализации на интерактивном экране (СПО ПОР)	3.2.10		
12.1	Проверка разграничения доступа	3.2.9.13	Методика № 124	
12.2	Проверка отображения на электронной карте местности закрытого сегмента подсистемы ПОР интегрированной обстановки в геоинформационной системе с возможностью вывода цифрового формуляра объекта с графическими и текстовыми документами	3.2.10.1	Методика № 125	
12.3	Проверка отображения и редактирования (при наличии прав доступа) на электронной карте местности геоинформационной системы закрытого сегмента подсистемы ПОР формуляра (наименование,	3.2.10.2	Методика № 126	

№ п/п	Наименование испытаний и проверок	Номер		Примечание
		пункта ТЗ, Дополнения №1 к ТЗ	методики испытаний	
	местонахождение, дополнительное описание и т.д.) при активации условного знака объекта			
12.4	Проверка нанесения интегрированной обстановки на электронную карту местности в геоинформационной системе	3.2.10.3	Методика № 127	
12.5	Проверка накопления информации в ручном режиме путем создания электронных формуляров объектов на электронной карте местности закрытого сегмента ПОР	3.2.10.4	Методика № 128	
12.6	Проверка нанесения оператором графической информации на электронную карту местности закрытого сегмента подсистемы ПОР в выбранный слой с использованием библиотеки условных знаков	3.2.10.5	Методика № 129	
12.7	Проверка экспорта в электронные документы и импорта файлов	3.2.10.6	Методика № 130	
12.8	Проверка визуального отображения демонстрируемой информации в многооконном режиме на средствах отображения информации	3.2.10.7	Методика № 131	
12.9	Проверка планирования и контроля выполнения мероприятий по информационному ограничению локального района	3.2.10.8	Методика № 132	
12.10	Проверка интегрированного представления различных видов	3.2.10.9	Методика № 133	

№ п/п	Наименование испытаний и проверок	Номер		Примечание
		пункта ТЗ, Дополнения №1 к ТЗ	методики испытаний	
	информации (текстовой, графической, аудио и видео)			
12.11	Проверка информационного обмена вышестоящих и подчиненных органов	3.2.10.11	Методика № 134	
12.12	Проверка автоматизированного взаимодействия с СПО подсистемы лингвистического обеспечения	3.2.10.12	Методика № 135	
12.13	Проверка обнаружения и предотвращения несанкционированной активности в режиме времени, близком к реальному	9.6	Методика № 136	
12.14	Проверка инвентаризации ресурсов и мониторинга изменений инфраструктуры	9.8, 9.9	Методика № 137	
12.15	Проверка сбора и анализа событий информационной безопасности, поступающих с контролируемых подсистем	9.10	Методика № 138	
12.16	Проверка визуализации полученных данных и оповещения администратора безопасности об инцидентах информационной безопасности	9.11	Методика № 139	
13	Проверка живучести и стойкости к внешним воздействиям	3.4, 3.4.1–3.4.2	Методика № 140	
14	Проверка надежности	3.5	Методика № 141	
15	Проверка эргономики, обитаемости и технической эстетики	3.6, 3.6.1–3.6.2	Методика № 142	
16	Проверка эксплуатации, хранения, удобства технического обслуживания и ремонта	3.7, 3.7.1	Методика № 143	

№ п/п	Наименование испытаний и проверок	Номер		Примечание
		пункта ТЗ, Дополнения №1 к ТЗ	методики испытаний	
17	Проверка безопасности	3.9, 3.9.1	Методика № 144	
18	Проверка обеспечения режима секретности, защиты от ИТР, степени секретности и класса защиты информации, технических средств обработки информации и требований защиты государственной тайны	3.10, 3.11, 9.3.1, 9.3.4, 9.3.5, 10	Методика № 145	
19	Проверка стандартизации, унификации и каталогизации	3.12, 3.12.1–3.12.4	Методика № 146	
20	Проверка конструктивных требований, требований к консервации, упаковке и маркировке	3.14, 3.14.1, 7, 7.1–7.2	Методика № 147	
21	Проверка технико-экономических требований	4.1–4.3	Методика № 148	
22	Проверка требований к диагностическому обеспечению	5.3, 5.3.1–5.3.4	Методика № 149	
23	Проверка требований к математическому, программному и информационно-лингвистическому обеспечению	5.4, 5.4.1–5.4.2.1, 5.4.2.4–5.4.3.3	Методика № 150	
24	Проверка требований к учебно-тренировочным средствам	8, 8.1–8.7	Методика № 151	
25	Проверка на патентную чистоту и патентоспособность изделия	9, 9.2	Методика № 152	
26	Проверка оценки соответствия защищенности ресурсов (сканирования на наличие уязвимостей) и устранения обнаруженных уязвимостей	9, 9.7	Методика № 153	
27	Проверка инвентаризации ресурсов	9, 9.8	Методика № 154	
28	Проверка мониторинга изменений инфраструктуры	9, 9.9	Методика № 155	
29	Проверка сбора и анализа	9, 9.10	Методика	

№ п/п	Наименование испытаний и проверок	Номер		Примечание
		пункта ТЗ, Дополнения №1 к ТЗ	методики испытаний	
	событий информационной безопасности, поступающих с контролируемых подсистем		№ 156	
30	Проверка визуализации полученных данных и оповещения администратора безопасности об инцидентах информационной безопасности	9, 9.11	Методика № 157	
31	Проверка отсутствия комментариев в скриптах и конфигурационных файлах, проверка скрытия национальной принадлежности, сведений о разработчике и Заказчике	9, 9.13	Методика № 158	
32	Проверка передачи данных о текущем состоянии с использованием устойчивых к обнаружению и компрометации протоколов	9, 9.15	Методика № 159	
33	Проверка защиты от MiTM-атак при организации информационного обмена	9, 9.16	Методика № 160	
34	Проверка регистрации и записи действий операторов	9, 9.17	Методика № 161	
35	Проверка исключения использования функциональных возможностей комплекса оператором в личных целях	9, 9.18	Методика № 162	
36	Проверка выполнения и приемки этапов СЧ ОКР	13.1–13.5.1, 13.7–13.10, 13.14–13.16	Методика № 163	

1.4.2 Изделие считается выдержавшим испытания по данным пунктам ТЗ, если результаты всех проверок, выполненных в соответствии с приведенным перечнем, – положительные.

1.4.3 По решению комиссии возможно проведение дополнительных испытаний, результаты которых отражаются в протоколе испытаний. Дополнительные испытания должны проводиться на основании требований ТЗ на СЧ ОКР.

1.5Условия, режимы, порядок, место проведения, виды и этапы испытаний

1.5.1 Порядок проведения предварительных испытаний определяется настоящим документом. Испытания проводятся в один этап на территории Исполнителя.

1.5.2 Перед проведением испытаний необходимо ознакомиться с документами:

– RU.BATC.00176-01 «Специальное программное обеспечение «Амезит-В». Спецификация»;

– RU.BATC.00176-01 91 01 «Специальное программное обеспечение «Амезит-В». Инструкция по защите информации от несанкционированного доступа»;

– RU.BATC.00176-01 92 01 «Специальное программное обеспечение «Амезит-В». Руководство администратора сети»;

– RU.BATC.00176-01 94 01 «Специальное программное обеспечение «Амезит-В». Руководство администратора безопасности»;

– RU.BATC.00176-01 95 01 «Специальное программное обеспечение «Амезит-В». Инструкция администратора безопасности»;

– RU.BATC.00176-01 96 01 «Специальное программное обеспечение «Амезит-В». Контрольный пример (методика) настройки СЗИ при эксплуатации изделия»;

– RU.BATC.00177-01 32 01 «Специальное программное обеспечение подсистемы формирования автономного сегмента сети передачи данных. Руководство системного программиста»;

– RU.BATC.00177-01 34 01 «Специальное программное обеспечение подсистемы формирования автономного сегмента сети передачи данных. Руководство оператора»;

– RU.BATC.00177-01 51 01 «Специальное программное обеспечение подсистемы формирования автономного сегмента сети передачи данных. Программа и методика испытаний»;

– RU.BATC.00177-01 92 01 «Специальное программное обеспечение подсистемы формирования автономного сегмента сети передачи данных. Руководство пользователя»;

– RU.ВАТС.00178-01 32 01 «Специальное программное обеспечение подсистемы контроля сообщений автономного сегмента сети передачи данных. Руководство системного программиста»;

– RU.ВАТС.00178-01 34 01 «Специальное программное обеспечение подсистемы контроля сообщений автономного сегмента сети передачи данных. Руководство оператора»;

– RU.ВАТС.00178-01 51 01 «Специальное программное обеспечение подсистемы контроля сообщений автономного сегмента сети передачи данных. Программа и методика испытаний»;

– RU.ВАТС.00178-01 92 01 «Специальное программное обеспечение подсистемы контроля сообщений автономного сегмента сети передачи данных. Руководство пользователя».

– RU.ВАТС.00179-01 32 01 «Специальное программное обеспечение подсистемы мониторинга сети Интернет и СМИ. Руководство системного программиста»;

– RU.ВАТС.00179-01 34 01 «Специальное программное обеспечение подсистемы мониторинга сети Интернет и СМИ. Руководство оператора»;

– RU.ВАТС.00179-01 51 01 «Специальное программное обеспечение подсистемы мониторинга сети Интернет и СМИ. Программа и методика испытаний»;

– RU.ВАТС.00179-01 92 01 «Специальное программное обеспечение подсистемы мониторинга сети Интернет и СМИ. Руководство пользователя».

– RU.ВАТС.00180-01 32 01 «Специальное программное обеспечение подсистемы анализа информационно-технических объектов телекоммуникационных систем. Руководство системного программиста»;

– RU.ВАТС.00180-01 34 01 «Специальное программное обеспечение подсистемы анализа информационно-технических объектов телекоммуникационных систем. Руководство оператора»;

– RU.ВАТС.00180-01 51 01 «Специальное программное обеспечение подсистемы анализа информационно-технических объектов телекоммуникационных систем. Программа и методика испытаний»;

– RU.ВАТС.00180-01 92 01 «Специальное программное обеспечение подсистемы анализа информационно-технических объектов телекоммуникационных систем. Руководство пользователя»;

– RU.ВАТС.00181-01 32 01 «Специальное программное обеспечение подсистемы первичного анализа информации. Руководство системного программиста»;

– RU.BATC.00181-01 34 01 «Специальное программное обеспечение подсистемы первичного анализа информации. Руководство оператора»;

– RU.BATC.00181-01 51 01 «Специальное программное обеспечение подсистемы первичного анализа информации. Программа и методика испытаний»;

– RU.BATC.00181-01 92 01 «Специальное программное обеспечение подсистемы первичного анализа информации. Руководство пользователя»;

– RU.BATC.00182-01 32 01 «Специальное программное обеспечение подсистемы ретрансляции данных с использованием промежуточных серверов. Руководство системного программиста»;

– RU.BATC.00182-01 34 01 «Специальное программное обеспечение подсистемы ретрансляции данных с использованием промежуточных серверов. Руководство оператора»;

– RU.BATC.00182-01 51 01 «Специальное программное обеспечение подсистемы ретрансляции данных с использованием промежуточных серверов. Программа и методика испытаний»;

– RU.BATC.00182-01 92 01 «Специальное программное обеспечение подсистемы ретрансляции данных с использованием промежуточных серверов. Руководство пользователя»;

– RU.BATC.00183-01 32 01 «Специальное программное обеспечение подсистемы подготовки, размещения и «раскрутки» специальных материалов. Руководство системного программиста»;

– RU.BATC.00183-01 34 01 «Специальное программное обеспечение подсистемы подготовки, размещения и «раскрутки» специальных материалов. Руководство оператора»;

– RU.BATC.00183-01 51 01 «Специальное программное обеспечение подсистемы подготовки, размещения и «раскрутки» специальных материалов. Программа и методика испытаний»;

– RU.BATC.00183-01 92 01 «Специальное программное обеспечение подсистемы подготовки, размещения и «раскрутки» специальных материалов. Руководство пользователя;

– RU.BATC.00184-01 32 01 «Специальное программное обеспечение подсистемы тестирования телекоммуникационного оборудования. Руководство системного программиста»;

– RU.BATC.00184-01 34 01 «Специальное программное обеспечение подсистемы тестирования телекоммуникационного оборудования. Руководство оператора»;

– RU.ВАТС.00184-01 51 01 «Специальное программное обеспечение подсистемы тестирования телекоммуникационного оборудования. Программа и методика испытаний»;

– RU.ВАТС.00184-01 92 01 «Специальное программное обеспечение подсистемы тестирования телекоммуникационного оборудования. Руководство пользователя».

– RU.ВАТС.00185-01 32 01 «Специальное программное обеспечение подсистемы хранения данных. Руководство системного программиста»;

– RU.ВАТС.00185-01 34 01 «Специальное программное обеспечение подсистемы хранения данных. Руководство оператора»;

– RU.ВАТС.00185-01 51 01 «Специальное программное обеспечение подсистемы хранения данных. Программа и методика испытаний»;

– RU.ВАТС.00185-01 92 01 «Специальное программное обеспечение подсистемы хранения данных. Руководство пользователя»;

– RU.ВАТС.00186-01 32 01 «Специальное программное обеспечение подсистемы обработки результатов и их визуализации на интерактивном экране. Руководство системного программиста»;

– RU.ВАТС.00186-01 34 01 «Специальное программное обеспечение подсистемы обработки результатов и их визуализации на интерактивном экране. Руководство оператора»;

– RU.ВАТС.00186-01 51 01 «Специальное программное обеспечение подсистемы обработки результатов и их визуализации на интерактивном экране. Программа и методика испытаний»;

– RU.ВАТС.00186-01 92 01 «Специальное программное обеспечение подсистемы обработки результатов и их визуализации на интерактивном экране. Руководство пользователя».

1.5.3 Испытания Изделия проводят в следующем порядке:

– проверка достаточности и полноты документации;

– проверка комплектности Изделия;

– проверка функциональных возможностей Изделия.

1.5.4 Проверка функциональных возможностей Изделия производится по следующему алгоритму:

– подключение аппаратно-программных средств к телекоммуникационной сети и сети электропитания;

– предварительная настройка (при необходимости) программных средств;

– проведение испытания в соответствии с выбранной методикой испытания;

– завершение испытаний с записью результатов в Протоколы предварительных испытания.

1.5.5 Испытания проводятся в нормальных климатических условиях:

– температура (20 ± 5) ºС;

– относительная влажность – (60 ± 15) % при атмосферном давлении (84 – 107) кПа (630 – 800) мм рт. ст.

1.6Материально-техническое обеспечение испытаний

1.6.1 Для проведения испытаний Заказчик предоставляет аппаратные и программные средства из состава аппаратно-программного комплекса (АПК) «Амезит».

1.6.2 Порядок настройки СПО, входящего в состав СПО «Амезит-В» приведен в следующих документах:

– RU.ВАТС.00176-01 91 01 «Специальное программное обеспечение «Амезит-В». Инструкция по защите информации от несанкционированного доступа»;

– RU.ВАТС.00176-01 92 01 «Специальное программное обеспечение «Амезит-В». Руководство администратора сети»;

– RU.ВАТС.00176-01 94 01 «Специальное программное обеспечение «Амезит-В». Руководство администратора безопасности»;

– RU.ВАТС.00176-01 95 01 «Специальное программное обеспечение «Амезит-В». Инструкция администратора безопасности»;

– RU.ВАТС.00176-01 96 01 «Специальное программное обеспечение «Амезит-В». Контрольный пример (методика) настройки СЗИ при эксплуатации изделия»;

– RU.ВАТС.00177-01 32 01 «Специальное программное обеспечение подсистемы формирования автономного сегмента сети передачи данных. Руководство системного программиста»;

– RU.ВАТС.00178-01 32 01 «Специальное программное обеспечение подсистемы контроля сообщений автономного сегмента сети передачи данных. Руководство системного программиста»;

– RU.ВАТС.00179-01 32 01 «Специальное программное обеспечение подсистемы мониторинга сети Интернет и СМИ. Руководство системного программиста»;

– RU.BATC.00180-01 32 01 «Специальное программное обеспечение подсистемы анализа информационно-технических объектов телекоммуникационных систем. Руководство системного программиста»;

– RU.BATC.00181-01 32 01 «Специальное программное обеспечение подсистемы первичного анализа информации. Руководство системного программиста»;

– RU.BATC.00182-01 32 01 «Специальное программное обеспечение подсистемы ретрансляции данных с использованием промежуточных серверов. Руководство системного программиста»;

– RU.BATC.00183-01 32 01 «Специальное программное обеспечение подсистемы подготовки, размещения и «раскрутки» специальных материалов. Руководство системного программиста»;

– RU.BATC.00184-01 32 01 «Специальное программное обеспечение подсистемы тестирования телекоммуникационного оборудования. Руководство системного программиста»;

– RU.BATC.00185-01 32 01 «Специальное программное обеспечение подсистемы хранения данных. Руководство системного программиста»;

– RU.BATC.00186-01 32 01 «Специальное программное обеспечение подсистемы обработки результатов и их визуализации на интерактивном экране. Руководство системного программиста».

1.6.3 Подключение аппаратных средств Изделия должно производиться в соответствии с схемами подключения (Приложение Б).

1.7Метрологическое обеспечение испытаний

1.7.1 Метрологическое обеспечение испытаний осуществляет Заказчик.

1.8Обеспечение защиты государственной тайны

1.8.1 Обеспечение защиты государственной тайны осуществляется в соответствии с документом «Инструкция по ЗИ от ИТР для этапа изготовления опытного образца».

1.9Отчетность

1.9.1 По окончании испытаний составляется акт предварительных испытаний и протоколы по пунктам ПМ.

1.9.2 Протоколы испытаний подписываются членами рабочей группы и членами комиссии, ответственными за проведение испытаний по данным пунктам программы. Протоколы утверждаются председателем комиссии.

1.9.3 По результатам предварительных испытаний составляют акт, на основании которого оформляют решение, где предусматривают выполнение мероприятий, обеспечивающих реализацию выводов и предложений,

указанных в акте. Если по результатам испытаний не требуется корректировка РКД и доработка опытного образца, решение по акту не оформляют, что должно быть отражено в акте, в этом случае акт утверждает генеральный директор ООО «НТЦ «Вулкан».

1.9.4 Акт предварительных испытаний оформляется в двух экземплярах с рассылкой в адрес ООО «НТЦ «Вулкан» и ФГУП «РНИИРС».

Приложение А

Методики испытаний

А.1 Методика № 1

А.1.1 В данной методике проводится проверка документации СПО «Амезит-В» на соответствие требованиям пунктов 5.1.1–5.1.4, 9.5, 13.2.5–13.2.6, 13.3, 13.5.1–13.5.8, 13.6.1, 13.11–13.13, 13.17–13.19 ТЗ на СЧ ОКР «Амезит-В».

А.1.2 В ходе проверки оценивается достаточность и полнота документации СПО «Амезит-В».

А.1.3 Для проведения проверки СПО «Амезит-В» на соответствие предъявляемым требованиям необходимо выполнить действия, описанные ниже.

А.1.3.1 Сравнить состава представленной документации с утвержденным перечнем программной документации и документом RU.ВАТС.00176-01 «Специальное программное обеспечение «Амезит-В». Спецификация». Убедиться, что представленный состав документации соответствует RU.ВАТС.00176-01 «Специальное программное обеспечение «Амезит-В». Спецификация».

А.1.3.2 Выполнить анализ содержания и оформления представленных документов на соответствие требованиям ГОСТ РВ 15.110-2003, ГОСТ РВ 15.203-2001, ГОСТ РВ 2.902-2005, ГОСТ РВ 15.211-2002, ГОСТ серии РВ 20.39.301-98–20.39.305-98, ГОСТ РВ 20.57.304-98, ОТТ 7.1.203-90, ГОСТ 2.601-2006 и ЕСПД.

А.1.3.3 Выполнить анализ эксплуатационной документации в части СПО технических средств анализа объектов телекоммуникационных систем и систем жизнеобеспечения, технических средств первичного анализа и технических средств формирования автономного сегмента сети передачи данных. Убедиться, что эксплуатационная документация разработана в легендированном виде и не содержать признаков ведомственной принадлежности.

А.1.4 СПО «Амезит-В» считается выдержавшим испытания по п. А.1.3.1–А.1.3.3 программы и методики испытаний и выполняющим пункты 5.1.1–5.1.4, 9.5, 13.2.5–13.2.6, 13.3, 13.5.1–13.5.8, 13.6.1, 13.11–13.13, 13.17–13.19 ТЗ на СЧ ОКР, если:

– представленная документация СПО «Амезит-В» по номенклатуре и количеству соответствует утвержденному перечню РКД документации и документу RU.ВАТС.00176-01 «Специальное программное обеспечение «Амезит-В». Спецификация»;

– представленная документация СПО «Амезит-В» соответствует по содержанию и оформлению требованиям ГОСТ РВ 15.110-2003, ГОСТ РВ 15.203-2001, ГОСТ РВ 2.902-2005, ГОСТ РВ 15.211-2002, ГОСТ серии РВ 20.39.301-98–20.39.305-98, ГОСТ РВ 20.57.304-98, ОТТ 7.1.203-90, ГОСТ 2.601-2006 и ЕСПД;

– разработаны и согласованы с головным исполнителем следующие документы по защите информации от НСД:

  - предложения в руководство администратора сети (описание процесса обработки информации, состава технических и программных средств, сопровождения (установка, настройка, эксплуатация) общего и специального программного обеспечения);
  - предложения в акт установки, настройки и функционирования общего программного обеспечения, специального программного обеспечения и средств защиты информации с протоколом подсчета контрольных сумм основных исполнительных файлов и динамических библиотек по выбранным критериям;

– разработаны следующие документы:

  - методика обновления интерфейсов сопряжения с внешними системами;
  - методика получения доступа к стороннему телекоммуникационному оборудованию в обход авторизации при наличии к нему физического доступа;
  - методика развертывания автономного сегмента сетей передачи данных;
  - перечень отчетных документов и формы их построения;
  - экранные формы графического интерфейса управления;
  - перечень конструкторской, эксплуатационной и программной документации;

– эксплуатационная документация в части СПО технических средств анализа объектов телекоммуникационных систем и систем жизнеобеспечения, технических средств первичного анализа и технических средств формирования автономного сегмента сети передачи данных разработана в легендированном виде и не содержит признаков ведомственной принадлежности.

A.2 Методика № 2

A.2.1 В данной методике проводится проверка состава СПО «Амезит-В» на соответствие требованиям пунктов 3.1, 5.4.2.2, 5.4.2.3, 9.14 ТЗ на СЧ ОКР «Амезит-В».

A.2.2 В ходе проверки оценивается комплектность СПО «Амезит-В».

A.2.3 Проверка выполняется сравнением фактического состава комплекта составных частей СПО «Амезит-В» с документом RU.BATC.00176-01 «Специальное программное обеспечение «Амезит-В». Спецификация».

A.2.4 СПО «Амезит-В» считается выдержавшим испытания по п. А.2.3 программы и методики испытаний и выполняющим пункты 3.1, 5.4.2.2, 9.14 ТЗ на СЧ ОКР, если:

- состав комплектов программного обеспечения, эксплуатационной и программной документации по номенклатуре соответствует документу RU.BATC.00176-01 «Специальное программное обеспечение «Амезит-В». Спецификация»;
- в состав ОПО входят:
  - операционные системы (ОС);
  - системы управления базами данных (СУБД);
  - драйверы, обеспечивающие работу периферийных устройств и корректную обработку различных видов информационных данных;
  - средства защиты информации (СЗИ), в том числе антивирусные средства (типа DrWeb или Антивирус Касперского);
- используемые средства антивирусной защиты (САВЗ) сертифицированы в системе сертификации средств защиты информации Минобороны России, проверены на возможность применения в изделии (в том числе на совместимость с программными и аппаратными средствами и соответствовать задаваемым требованиям по антивирусной защите) и включены в состав программных средств изделия установленным порядком;
- ОПО изделия функционирует и обеспечивает организацию вычислительного процесса на вычислительных средствах системы;
- в ОПО присутствуют средства контроля целостности ПО.

A.3 Методика № 3

A.3.1 В данной методике проводится проверка СПО ПАС на соответствие требованиям пунктов 3.2.1, 3.2.1.1 ТЗ на СЧ ОКР «Амезит-В».

А.3.2 В соответствии с требованиями пунктов 3.2.1, 3.2.1.1 ТЗ на СЧ ОКР «Амезит-В» СПО ПАС должно обеспечивать ретрансляцию трафика и организацию подключения к следующим проводным линиям связи:

- Ethernet;
- GPON;
- DOCSIS;
- ADSL (DSLAM).

А.3.3 Для проведения проверки СПО ПАС на соответствие предъявляемым требованиям необходимо выполнить действия, описанные ниже.

А.3.3.1 Собрать испытательный стенд в соответствии со схемой на рисункеРисунок 3.

А.3.3.2 Выполнить поочередное подключение генератора трафика (АПК СКАТ) к испытательному стенду с использованием проводных линий связи разных типов: Ethernet, GPON, DOCSIS, ADSL (DSLAM). Порядок подключения генератора трафика (АПК СКАТ) приведен в документе RU.ВАТС.00177-01 32 01 «Специальное программное обеспечение подсистемы формирования автономного сегмента сети передачи данных. Руководство системного программиста».

А.3.3.3 Выполнить запуск генератора трафика (АПК СКАТ) для обеспечения устойчивого трафика (передается файл testdata15m размером 15 Мб), проходящего через испытательный стенд. Порядок запуска и настройки генератора трафика (АПК СКАТ) приведен в документе RU.ВАТС.00177-01 32 01 «Специальное программное обеспечение подсистемы формирования автономного сегмента сети передачи данных. Руководство системного программиста».

А.3.3.4 С АРМ оператора ПАС запустить ПО управления маршрутизатора D-link DGS-1100-24 (выполнить вход в консоль управления). Инструкции по работе с маршрутизатором приведены в документе RU.ВАТС.00177-01 32 01 «Специальное программное обеспечение подсистемы формирования автономного сегмента сети передачи данных. Руководство системного программиста».

А.3.3.5 Просмотреть статистику соединений маршрутизатора D-link DGS-1100-24. Убедиться, что количество байт, поступивщих на порт маршрутизатора (порт 2) (от генератора трафика (АПК СКАТ)) равно кол-ву байт трафика, транслированного через выходной порт маршрутизатора D-link DGS-1100-24 (порт 22). Порядок просмотра статистики приведен в документе RU.ВАТС.00177-01 32 01 «Специальное программное обеспечение подсистемы

формирования автономного сегмента сети передачи данных. Руководство системного программиста».

А.3.4 СПО ПАС считается выдержавшим испытания по п. А.3.3.1-А.3.3.5 программы и методики испытаний и выполняющим пункты 3.2.1, 3.2.1.1 на СЧ ОКР, если испытательный стенд обеспечивает ретрансляцию трафика (кол-во байт, поступивших на входной порт равно кол-ву байт трафика, переданного на выходной порт маршрутизатора D-link DGS-1100-24 (15 Мб)) для всех вариантов подключения генератора трафика при помощи перечисленных типов проводных линий связи: Ethernet, GPON, DOCSIS, ADSL (DSLAM).

А.4 Методика № 4

А.4.1 В данной методике проводится проверка СПО ПАС на соответствие требованиям пунктов 3.2.1, 3.2.1.2 ТЗ на СЧ ОКР «Амезит-В».

А.4.2 В соответствии с требованиями пунктов 3.2.1, 3.2.1.2 ТЗ на СЧ ОКР «Амезит-В» СПО ПАС должно обеспечивать:

- ретрансляцию трафика с использованием беспроводных линий связи:
  - GSM;
  - GPRS;
  - EDGE;
- организацию подключения к следующим беспроводным сетям связи:
  - GSM;
  - GPRS;
  - LTE;
  - CDMA;
  - Wi-Fi;
  - WiMAX.

А.4.3 Для проведения проверки СПО ПАС на соответствие предъявляемым требованиям необходимо выполнить действия, описанные ниже.

А.4.3.1 Собрать испытательный стенд в соответствии со схемой на рисунке Рисунок 3.

А.4.3.2 Выполнить поочередное подключение генератора трафика (АПК СКАТ) к испытательному стенду с использованием беспроводных линий связи разных типов: GSM, GPRS, LTE, CDMA, Wi-Fi, WiMAX. Со стороны стенда следует модемы беспроводных устройств подключать к порту 3 маршрутизатора D-link DGS-1100-24.

А.4.3.3 Выполнить запуск генератора трафика (АПК СКАТ) для обеспечения устойчивого трафика (передается файл testdata25M размером 25 Мб). Порядок запуска и настройки генератора трафика (АПК СКАТ) приведен в документе RU.BATC.00177-01 32 01 «Специальное программное обеспечение подсистемы формирования автономного сегмента сети передачи данных. Руководство системного программиста».

А.4.3.4 С АРМ оператора ПАС запустить ПО управления маршрутизатора D-link DGS-1100-24 (выполнить вход в консоль управления). Инструкции по работе с маршрутизатором приведены в документе RU.BATC.00177-01 32 01 «Специальное программное обеспечение подсистемы формирования автономного сегмента сети передачи данных. Руководство системного программиста».

А.4.3.5 Просмотреть статистику маршрутизатора D-link DGS-1100-24. Убедиться, что кол-во байт, поступивщих на порт 3 маршрутизатора равно кол-ву байт трафика, транслированного через выходной порт 22 маршрутизатора D-link DGS-1100-24 (25 Мб).

А.4.3.6 Имитировать трафик со стороны мобильного устройства, путем запуска имитатора виртуальной базовой станции (передается файл testdata35M размером 35 Мб). Имитатор базовой станции должен быть подключен к порту 4 маршрутизатора D-link DGS-1100-24. Инструкции по подключению имитатора ВБС и созданию трафика приведены в документах RU.BATC.00177-01 32 01 «Специальное программное обеспечение подсистемы формирования автономного сегмента сети передачи данных. Руководство системного программиста» и RU.BATC.00177-01 32 06 «Специальное программное обеспечение подсистемы формирования автономного сегмента сети передачи данных. Программное обеспечение управления базовой станцией. Руководство системного программиста».

А.4.3.7 С АРМ оператора ПАС запустить ПО управления маршрутизатора D-link DGS-1100-24 (выполнить вход в консоль управления). Инструкции по работе с маршрутизатором приведены в документе RU.BATC.00177-01 32 01 «Специальное программное обеспечение подсистемы формирования автономного сегмента сети передачи данных. Руководство системного программиста».

А.4.3.8 Просмотреть статистику маршрутизатора D-link DGS-1100-24. Убедиться, что кол-во байт, поступивщих на порт 4 маршрутизатора равно кол-ву байт трафика, транслированного через выходной порт 22 маршрутизатора D-link DGS-1100-24 (35 Мб).

А.4.4 СПО ПАС считается выдержавшим испытания по п. А.4.3.1-А.4.3.8 программы и методики испытаний и выполняющим пункты 3.2.1, 3.2.1.2 на СЧ ОКР, если:

- испытательный стенд обеспечивает ретрансляцию трафика с использованием беспроводных линий связи разных типов: GSM, GPRS, LTE, CDMA, Wi-Fi, WiMAX (объем входного трафика для каждого варианта подключения равен объему выходного трафика 25 Мб);
- испытательный стенд обеспечивает ретрансляцию трафика со стороны имитатора виртуальной базовой станции (объем входного трафика равен объему выходного трафика 35 Мб).

А.5 Методика № 5

А.5.1 В данной методике проводится проверка СПО ПАС на соответствие требованиям пунктов 3.2.1, 3.2.1.3 ТЗ на СЧ ОКР «Амезит-В».

А.5.2 В соответствии с требованиями пунктов 3.2.1, 3.2.1.3 ТЗ на СЧ ОКР «Амезит-В» СПО ПАС должно обеспечивать управление сторонним телекоммуникационным оборудованием уровня распределения и уровня ядра без авторизации и при наличии к нему физического доступа для следующих моделей оборудования:

- Huawei серии S5XXX;
- Juniper серий MX40, MX80, MX10, MX104;
- Cisco серий 2000, 2500, 3000, 680x0-Based 4000, 7000;
- Extreme Networks Summit серий x430, x440, x450, x460;
- D-Link серий DGS-3627, DGS-3620-28, DES-3200-10, DES-3200-24.

А.5.3 Для проведения проверки СПО ПАС на соответствие предъявляемым требованиям необходимо выполнить действия, описанные ниже.

А.5.3.1 Собрать испытательный стенд в соответствии со схемой на рисунке Рисунок 3.

А.5.3.2 Подключить АРМ оператора ПАС получения доступа к коммутатору D-link DGS-1100-24 через интерфейс RS-232. Инструкции по подключению приведены в документе RU.BATC.00177-01 32 01 «Специальное программное обеспечение подсистемы формирования автономного сегмента сети передачи данных. Руководство системного программиста».

А.5.3.3 На АРМ оператора ПАС выполнить запуск утилиты командной строки Terminal. Во время загрузки при появлении в консоли сообщения: Please wait, loading V6.20.B18 Runtime image .... 100 %, требуется

многократно нажать shift+6+3 до получения сообщения в консоли: Factory Default Enable...

А.5.3.4 После того, как D-link DGS-1100-24 произведет загрузку, вести команду reset config и произвести сохранение настроек командой save.

А.5.3.5 После перезагрузки маршрутизатора выполнить с АРМ оператора ПАС подключение к маршрутизатору D-link DGS-1100-24 (запустить утилиту Terminal). Убедится, что выполняется вход в командную строку маршрутизатора «>». Выполнить установку нового пароля «12345».

А.5.3.6 На АРМ оператора ПАС выполнить настройку ПО получения доступа (согласно заводским настройкам) для модели D-link DGS-1100-24.

А.5.3.7 Для проверки программного способа получения доступа к оборудованию на АРМ оператора ПАС запустить ПО получения доступа, указав в качестве параметра IP-адрес 10.10.10.113 маршрутизатора D-link DGS-1100-24. Порядок получения доступа приведен в документе RU.BATC.00177-01 92 02 «Специальное программное обеспечение подсистемы формирования автономного сегмента сети передачи данных. Программное обеспечение получения доступа. Руководство пользователя».

А.5.3.8 Просмотреть результаты работы ПО получения доступа. Убедиться, что были сформированы записи, содержащие парольную информацию для доступа к консоли управления маршрутизатора D-link DGS-1100-24, найден пароль - «12345». Порядок просмотра результатов приведен в документе RU.BATC.00177-01 92 02 «Специальное программное обеспечение подсистемы формирования автономного сегмента сети передачи данных. Программное обеспечение получения доступа. Руководство пользователя».

А.5.3.9 На АРМ оператора ПАС выполнить поочередную настройку ПО получения доступа (согласно заводским настройкам) для следующих моделей оборудования:

- Huawei серии S5XXX;
- Juniper серий MX40, MX80, MX10, MX104;
- Cisco серий 2000, 2500, 3000, 680x0-Based 4000, 7000;
- Extreme Networks Summit серий x430, x440, x450, x460;
- D-Link серий DGS-3627, DGS-3620-28, DES-3200-10, DES-3200-24.

А.5.3.10 На АРМ оператора ПАС выполнить поочередный запуск ПО получения доступа для перечисленных моделей оборудования. Инструкции по запуску и настройке приведены в документе RU.BATC.00177-01 92 02 «Специальное программное обеспечение подсистемы формирования автономного сегмента сети передачи данных. Программное обеспечение получения доступа. Руководство пользователя».

А.5.4 СПО ПАС считается выдержавшим испытания по п. А.5.3.1-А.5.3.10 программы и методики испытаний и выполняющим пункты 3.2.1, 3.2.1.3 на СЧ ОКР, если пользователь, выполнив процедуру физического подключения через интерфейс RS-232, смог установить новый пароль на устройство, а также при помощи ПО получения доступа смог получить парольную информацию (пароль «12345»), обеспечивающую вход в ПО управления сетевым устройством по адресу 10.10.10.113 (маршрутизатор D-link DGS-1100-24).

А.6 Методика № 6

А.6.1 В данной методике проводится проверка СПО ПАС на соответствие требованиям пунктов 3.2.1, 3.2.1.4 ТЗ на СЧ ОКР «Амезит-В».

А.6.2 В соответствии с требованиями пунктов 3.2.1, 3.2.1.4 ТЗ на СЧ ОКР «Амезит-В» СПО ПАС должно обеспечивать сбор, регистрацию и отображение следующей информации:

А.6.2.1 В части работы контролируемого оборудования, обладающего возможностью сбора и предоставления своей диагностической информации:

- состояние (работает/не работает);
- версия ОС;
- записи журнала событий;
- показатели нагрузки на оборудование.

Примечание. Под контролируемым оборудованием здесь и далее понимаются аппаратные средства подсистемы ПАС и телекоммуникационное оборудование третьих фирм, подключенные к АПК «Амезит» (при получении доступа к нему).

А.6.2.2 В части трафика, проходящего через контролируемое оборудование, обладающее возможностью сбора и предоставления информации по трафику с использованием протокола NetFlow:

- дата и время начала соединения;
- дата и время завершения соединения;
- информация о клиенте (IP-адрес, доменное имя (при наличии), порт);
- информация о сервере (IP-адрес, доменное имя (при наличии), порт);
- код протокола в соответствии с RFC1700.

А.6.2.3 Таблиц маршрутизации контролируемого оборудования.

А.6.3 Для проведения проверки СПО ПАС на соответствие предъявляемым требованиям необходимо выполнить действия, описанные ниже.

А.6.3.1 Собрать испытательный стенд в соответствии со схемой на рисунке Рисунок 3.

А.6.3.2 Выполнить вход в интерфейс СПО управления ПАС, перейдя в раздел просмотра параметров контролируемого оборудования. Инструкция по просмотру параметров контролируемого оборудования приведена в документе RU.BATC.00177-01 92 05 «Специальное программное обеспечение подсистемы формирования автономного сегмента сети передачи данных. Программное обеспечение диагностики и управления. Руководство пользователя».

А.6.3.3 Просмотреть параметры сервера ServWin1.

А.6.3.4 СПО ПАС считается выдержавшим испытания по п. А.6.3.1-А.6.3.3 программы и методики испытаний и выполняющим пункты 3.2.1, 3.2.1.4 на СЧ ОКР, если пользователь в интерфейсе ПО диагностики и управления в разделе просмотра параметров контролируемого оборудования наблюдает диагностическую информацию о работе оборудования:

- состояние (Активировано);
- версия ОС (Windows 10);
- нагрузка на подсистему в виде графика CPU Load, Traffic on Eth1;
- журнал событий (Auth, Syslog, Messages, Application, Security, System).

А.6.3.5 С АРМ оператора ПАС запустить обозреватель и выполнить вход в интерфейс оператора ПО мониторинга сетевого трафика, перейдя в раздел просмотра статистики соединений. Инструкция по работе с ПО мониторинга сетевого трафика приведена в документах RU.BATC.00177-01 92 07 «Специальное программное обеспечение подсистемы формирования автономного сегмента сети передачи данных. Программное обеспечение мониторинга сетевого трафика. Руководство пользователя»

А.6.3.6 Просмотреть журнал соединений.

А.6.4 СПО ПАС считается выдержавшим испытания по п. А.6.3.5-А.6.3.6 программы и методики испытаний и выполняющим пункты 3.2.1, 3.2.1.4 на СЧ ОКР, если пользователь в интерфейсе ПО мониторинга трафика в разделе просмотра статистики соединений может видеть записи журнала соединений:

- дата и время начала соединения, вида: 11.05.2018 14:31;
- дата и время завершения соединения, вида: 11.05.2018 14:41;
- информация о клиенте вида: 31.132.105.110: 21;
- информация о сервере вида: 87.242.79.110: 1358;
- код протокола либо номер порта для TCP/UDP, вида: FTP:
- размер переданных данных, вида: 10084.

А.6.4.1 С АРМ оператора ПАС запустить обозреватель и выполнить вход в интерфейс оператора ПО мониторинга сетевого трафика, перейдя в раздел просмотра информации о маршрутах. Инструкция по работе с ПО

мониторинга сетевого трафика приведена в документах RU.BATC.00177-01 92 07 «Специальное программное обеспечение подсистемы формирования автономного сегмента сети передачи данных. Программное обеспечение мониторинга сетевого трафика. Руководство пользователя».

А.6.4.2 С АРМ оператора ПАС запустить обозреватель, зайти в ПО управления маршрутизатором D-link DGS-1100-24 и посмотреть информацию о маршрутах на маршрутизаторе. Убедиться, что для контролируемого оборудования выполняется сбор диагностической информации по маршрутам проходящего трафика и отображение маршрутной информации в виде таблиц маршрутизации. Порядок просмотра статистики приведен в документе RU.BATC.00177-01 34 07 «Специальное программное обеспечение подсистемы формирования автономного сегмента сети передачи данных. Программное обеспечение мониторинга сетевого трафика. Руководство пользователя».

А.6.5 СПО ПАС считается выдержавшим испытания по п. А.6.4.1-А.6.4.2 программы и методики испытаний и выполняющим пункты 3.2.1, 3.2.1.4 на СЧ ОКР, если пользователь в интерфейсе ПО диагностики и управления в разделе просмотра параметров контролируемого оборудования наблюдает содержимое таблицы маршрутизации, вида:

```
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
192.168.0.0     0.0.0.0         255.255.255.0   U     0      0        0 eth0
10.10.10.1         192.168.0.1     0.0.0.0         UG    0      0        0 eth0
```

А.7 Методика № 7

А.7.1 В данной методике проводится проверка СПО ПАС на соответствие требованиям пунктов 3.2.1, 3.2.1.5 ТЗ на СЧ ОКР «Амезит-В».

А.7.2 В соответствии с требованиями пунктов 3.2.1, 3.2.1.5 ТЗ на СЧ ОКР «Амезит-В» СПО ПАС должно обеспечивать маршрутизацию трафика и передачу его на технические средства первичного анализа информации.

А.7.3 Для проведения проверки СПО ПАС на соответствие предъявляемым требованиям необходимо выполнить действия, описанные ниже.

А.7.3.1 Выполнить подключение генератора трафика (АПК СКАТ) к испытательному стенду. Порядок настройки испытательного стенда приведен в документе RU.BATC.00177-01 32 01 «Специальное программное обеспечение подсистемы формирования автономного сегмента сети передачи данных. Руководство системного программиста».

А.7.3.2 Выполнить запуск генератора трафика (АПК СКАТ), который обеспечивает устойчивый трафик (передается файл testdata25M размером 25 МБ со скоростью 100 Мбит/с). Порядок запуска и настройки генератора

трафика приведен в документе RU.ВАТС.00177-01 32 01 «Специальное программное обеспечение подсистемы формирования автономного сегмента сети передачи данных. Руководство системного программиста».

А.7.3.3 С АРМ оператора ПАС выполнить вход в консоль управления маршрутизатора D-link DGS-1100-24. Инструкции по работе с маршрутизатором D-link DGS-1100-24 приведены в документе RU.ВАТС.00177-01 32 01 «Специальное программное обеспечение подсистемы формирования автономного сегмента сети передачи данных. Руководство системного программиста».

А.7.3.4 Просмотреть статистику маршрутизатора D-link DGS-1100-24 по порту 19 (к которому подключен сервер ППА). Убедиться, что обеспечивается маршрутизация трафика (пакеты трафика достигают порта 19 маршрутизатора D-link DGS-1100-24).

А.7.3.5 Просмотреть статистику маршрутизатора D-link DGS-1100-24. Убедиться, что выполняется передача трафика на технические средства первичного анализа информации (сервер «СКАТ съема и анализа трафика»), объем трафика, проходящего через порт 19 равен 25 Мб, скорост трафика составляет 100 Мбит/с.

А.7.4 СПО ПАС считается выдержавшим испытания по п. А.7.3.1-А.7.3.5 программы и методики испытаний и выполняющим пункты 3.2.1, 3.2.1.5 на СЧ ОКР, если обеспечивается маршрутизация и передача трафика (кол-во байт передаваемого файла равно кол-ву байт трафика, поступившего на оборудование ППА (25 МБ)) со скоростью 100 Мбит/с.

А.8 Методика № 8

А.8.1 В данной методике проводится проверка СПО ПАС на соответствие требованиям пунктов 3.2.1, 3.2.1.6 ТЗ на СЧ ОКР «Амезит-В».

А.8.2 В соответствии с требованиями пунктов 3.2.1, 3.2.1.6 ТЗ на СЧ ОКР «Амезит-В» СПО ПАС должно обеспечивать автоматическую настройку сети с использованием протоколов DHCP, NTP, DNS.

А.8.3 Для проведения проверки СПО ПАС на соответствие предъявляемым требованиям необходимо выполнить действия, описанные ниже.

А.8.3.1 Собрать испытательный стенд в соответствии со схемой на рисунке Рисунок 3.

А.8.3.2 Выполнить включение АРМ оператора ПАС.

А.8.3.3 Просмотреть параметры сетевого соединения АРМ оператора. Убедиться, что выполнена автоматическая настройка IP-адреса с

использованием протокола DHCP. Порядок просмотра параметров сетевого соединения АРМ приведен в документе RU.BATC.00177-01 32 01 «Специальное программное обеспечение подсистемы формирования автономного сегмента сети передачи данных. Руководство системного программиста».

А.8.4 СПО ПАС считается выдержавшим испытания по п. А.8.3.1-А.8.3.3 программы и методики испытаний и выполняющим пункты 3.2.1, 3.2.1.6 на СЧ ОКР, если при включении АРМ оператора ПАС в автономный сегмент выполнена автоматическая настройка IP адреса:

```
C:\Users>ipconfig /all
Настройка протокола IP для Windows
Ethernet adapter Ethernet:
DNS-суффикс подключения . . . . . : domenpc.ru
Описание. . . . . . . . . . . . . : Intel(R) Ethernet Connection I219-V
 Физический адрес. . . . . . . . . : 40-8D-5C-C9-41-17
 DHCP включен. . . . . . . . . . . : Да
 Автонастройка включена. . . . . . : Да
 IPv4-адрес. . . . . . . . . . . . : 10.0.6.146(Основной)
 Маска подсети . . . . . . . . . . : 255.255.255.0
```

А.8.4.1 Просмотреть параметры службы точного времени АРМ оператора ПАС. Убедиться, что выполнена автоматическая настройка синхронизации времени АРМ оператора ПАС с использованием протокола NTP. Порядок просмотра параметров службы точного времени АРМ приведен в документе
RU.BATC.00177-01 32 01 «Специальное программное обеспечение подсистемы формирования автономного сегмента сети передачи данных. Руководство системного программиста».

А.8.5 СПО ПАС считается выдержавшим испытания по п. А.8.4.1 программы и методики испытаний и выполняющим пункты 3.2.1, 3.2.1.6 на СЧ ОКР, если при включении АРМ оператора ПАС выполнена автоматическая синхронизация времени:

```
C:\Users>w32tm /query /peers
#Узлы: 1
Узел партнера: dc03.domenpc.ru
Состояние: Активный
Осталось времени: 18125.1491263s
Режим: 3 (Клиент)
Страта: 4 (вторичная ссылка - синхронизирована с помощью (S)NTP)
ОдноранговыйИнтервал опроса: 15 (32768s)
УзелИнтервал опроса: 15 (32768s)
```

А.8.5.1 Выполнить DNS-запрос с помощью командной строки АРМ оператора ПАС и просмотреть результаты. Убедиться, что выполняется автоматическая трансляция доменных имен ресурсов в IP-адреса с использованием протокола DNS. Порядок выполнения DNS-запроса приведен в

документе RU.BATC.00177-01 32 01 «Специальное программное обеспечение подсистемы формирования автономного сегмента сети передачи данных. Руководство системного программиста».

А.8.6 СПО ПАС считается выдержавшим испытания по п. А.8.5.1 программы и методики испытаний и выполняющим пункты 3.2.1, 3.2.1.6 на СЧ ОКР, если при включении АРМ оператора ПАС выполняется автоматическая трансляция доменных имен ресурсов в IP-адреса с использованием протокола DNS:

```
C:\Users>nslookup mail.ru
dc03.domenpc.ru
Address:  10.0.0.20
```

А.9 Методика № 9

А.9.1 В данной методике проводится проверка СПО ПАС на соответствие требованиям пунктов 3.2.1, 3.2.1.7 ТЗ на СЧ ОКР «Амезит-В».

А.9.2 В соответствии с требованиями пунктов 3.2.1, 3.2.1.7 ТЗ на СЧ ОКР «Амезит-В» СПО ПАС должно обеспечивать приоритизацию трафика с использованием TOS.

А.9.3 Для проведения проверки СПО ПАС на соответствие предъявляемым требованиям необходимо выполнить действия, описанные ниже.

А.9.3.1 Собрать испытательный стенд в соответствии со схемой на рисунке Рисунок 2.

А.9.3.2 Выполнить подключение генератора трафика (АПК СКАТ) к испытательному стенду. Порядок подключения генератора трафика (АПК СКАТ) и настройки испытательного стенда приведен в документе RU.BATC.00177-01 32 01 «Специальное программное обеспечение подсистемы формирования автономного сегмента сети передачи данных. Руководство системного программиста».

А.9.3.3 Выполнить вход в интерфейс оператора ПО управления генератором трафика (АПК СКАТ) и выполнить настройку генератора трафика в соответствии со следующими условиями: генерируемый трафик состоит из двух протоколов (http и ftp), соотношение протоколов в трафике: 50 % http на 50 % ftp к объему создаваемого трафика, создаваемый трафик занимает полосу пропускания маршрутизатора испытательного стенда D-link DGS-1100-24 (100 Мбит/с). Порядок запуска и настройки генератора трафика (АПК СКАТ) приведен в документе RU.BATC.00177-01 32 01 «Специальное программное обеспечение подсистемы формирования автономного сегмента сети передачи данных. Руководство системного программиста».

А.9.3.4 Выполнить запуск генерации трафика.

А.9.3.5 С АРМ оператора ПАС выполнить вход в консоль управления маршрутизатора D-link DGS-1100-24. Инструкции по работе с маршрутизатором приведены в документе RU.ВАТС.00177-01 32 01 «Специальное программное обеспечение подсистемы формирования автономного сегмента сети передачи данных. Руководство системного программиста».

А.9.3.6 Просмотреть статистику маршрутизатора D-link DGS-1100-24. Убедиться, что обеспечивается поступление трафика с соотношением между протоколами в трафике 50 % http на 50 % ftp.

А.9.3.7 С АРМ оператора ПАС выполнить вход в консоль управления маршрутизатора D-link DGS-1100-24, перейти в раздел настройки приоритетов трафика и установить приоритет для трафика по протоколу http в 80 %, а для протокола ftp – в 20 % от полосы пропускания.

А.9.3.8 Просмотреть статистику маршрутизатора D-link DGS-1100-24. Убедиться, что трафик протокола http проходит без ограничений, скорость прохождения трафика по протоколу ftp упала в соответствии с выделенной полосой пропускания до 20 Мбит/с.

А.9.4 СПО ПАС считается выдержавшим испытания по п. А.9.3.1-А.9.3.8 программы и методики испытаний и выполняющим пункты 3.2.1, 3.2.1.7 на СЧ ОКР, если обеспечивается управление приоритизацией трафика: для протокола http скорость изменилась с 50 Мбит/с до 80 Мбит/с, а для протокола ftp скорость изменилась с 50 Мбит/с до 20 Мбит/с.

А.10 Методика № 10

А.10.1 В данной методике проводится проверка СПО ПАС на соответствие требованиям пунктов 3.2.1, 3.2.1.8 ТЗ на СЧ ОКР «Амезит-В».

А.10.2 В соответствии с требованиями пунктов 3.2.1, 3.2.1.8 ТЗ на СЧ ОКР «Амезит-В» СПО ПАС должно обеспечивать балансировку нагрузки с динамическим распределением ресурсов.

А.10.3 Для проведения проверки СПО ПАС на соответствие предъявляемым требованиям необходимо выполнить действия, описанные ниже.

А.10.3.1 Собрать испытательный стенд в соответствии со схемой на рисунке Рисунок 3.

А.10.3.2 С АРМ оператора ПАС войти в консоль управления маршрутизатора D-link DGS-1100-24, посредством которого испытательный стенд подключен к сети Интернет. Инструкции по работе с маршрутизатором

приведены в документе RU.BATC.00177-01 32 01 «Специальное программное обеспечение подсистемы формирования автономного сегмента сети передачи данных. Руководство системного программиста».

А.10.3.3 Выполнить настройку подключения испытательного стенда к сети Интернет, при которой испытательный стенд подключен к сети Интернет при помощи двух каналов связи.

А.10.3.4 Выполнить запуск генератора трафика (АПК СКАТ), который обеспечивает устойчивый трафик к ресурсам, расположенным в сети Интернет. Порядок запуска и настройки генератора трафика приведен в документе RU.BATC.00177-01 32 01 «Специальное программное обеспечение подсистемы формирования автономного сегмента сети передачи данных. Руководство системного программиста».

А.10.3.5 Выполнить вход в интерфейс оператора СПО ПАС, перейдя в раздел просмотра статистики трафика, проходящего через интерфейсы маршрутизатора D-link DGS-1100-24 (порт 2 и порт 3).

А.10.3.6 Просмотреть статистику. Убедиться, что используются оба канала, соединяющих испытательный стенд с сетью Интернет. Порядок просмотра статистики приведен в документе RU.BATC.00177-01 34 07 «Специальное программное обеспечение подсистемы формирования автономного сегмента сети передачи данных. Программное обеспечение мониторинга сетевого трафика. Руководство пользователя».

А.10.3.7 Смоделировать ситуацию недоступности одного из каналов связи (путем физического отключения канала связи или путем логического отключения сетевого интерфейса в консоли управления маршрутизатора D-link DGS-1100-24 (порт 3)).

А.10.3.8 Выполнить вход в СПО мониторинга сетевого трафика, перейдя в раздел просмотра статистики трафика, проходящего через интерфейсы маршрутизатора D-link DGS-1100-24.

А.10.3.9 Просмотреть статистику по портам 2 и 3. Убедиться, что выполняется автоматическая балансировка нагрузки, при недоступности одного из каналов связи для передачи всего трафика используется оставшийся канал связи. Порядок просмотра статистики приведен в документе RU.BATC.00177-01 34 07 «Специальное программное обеспечение подсистемы формирования автономного сегмента сети передачи данных. Программное обеспечение мониторинга сетевого трафика. Руководство пользователя».

А.10.4 СПО ПАС считается выдержавшим испытания по п. А.10.3.1-А.10.3.9 программы и методики испытаний и выполняющим пункты 3.2.1, 3.2.1.8 на СЧ ОКР, если: статистика распределения сетевого трафика по

сетевым каналам изменилась от значения 50 Мбит/с для первого сетевого канала (порт 2) и 50 Мбит/с для второго сетевого канала (порт 3) до значения 100Мбит/с для первого сетевого канала (порт 2) и на 0 Мбит/с для второго сетевого канала (порт 3) (автоматическое перенаправление всего трафика на работающий канал связи).

А.11 Методика № 11

А.11.1 В данной методике проводится проверка СПО ПАС на соответствие требованиям пунктов 3.2.1, 3.2.1.9 ТЗ на СЧ ОКР «Амезит-В».

А.11.2 В соответствии с требованиями пунктов 3.2.1, 3.2.1.9 ТЗ на СЧ ОКР «Амезит-В» СПО ПАС должно обеспечивать автоматизированное управление модулями ретрансляции с предоставлением единого графического интерфейса.

А.11.3 Для проведения проверки СПО ПАС на соответствие предъявляемым требованиям необходимо выполнить действия, описанные ниже.

А.11.3.1 Собрать испытательный стенд в соответствии со схемой на рисунке Рисунок 3.

А.11.3.2 Выполнить вход в единый графический интерфейс оператора СПО ПАС, перейдя в раздел автоматизированного управления сетевыми устройствами (модулями ретрансляции). Инструкции по работе с ПО диагностики и управления приведены в документах RU.ВАТС.00177-01 34 05 «Специальное программное обеспечение подсистемы формирования автономного сегмента сети передачи данных. Программное обеспечение диагностики и управления. Руководство системного программиста» и RU.ВАТС.00177-01 92 05 «Специальное программное обеспечение подсистемы формирования автономного сегмента сети передачи данных. Программное обеспечение диагностики и управления. Руководство пользователя».

А.11.3.3 Выбрать телекоммуникационное устройство (маршрутизатор D-link DGS-1100-24), убедиться, что СПО ПАС показывает список скриптов управления и перейти в форму настройки нового скрипта.

А.11.3.4 В форме создания нового скрипта указать наименование скрипта и файл, содержащий команды настройки сетевого устройства (изменение IP-адреса сервера ServWin1).

А.11.3.5 Сохранить новый скрипт.

А.11.3.6 Выполнить возврат в форму просмотра списка сетевых устройств.

A.11.3.7 Повторно выбрать сервер ServWin1 и дать команду показать список доступных скриптов управления.

A.11.3.8 Просмотреть скрипты управления. Убедиться, что в списке доступных скриптов управления присутствует скрипт изменения IP-адреса, который был создан на предыдущем шаге.

A.11.3.9 Выбрать скрипт изменения IP-адреса и дать команду на его выполнение.

A.11.3.10 Дождаться появления сообщения, что скрипт выполнен.

A.11.3.11 С АРМ оператора ПАС выполнить вход в консоль управления сервера ServWin1.

A.11.3.12 Запустить командную строку сервера ServWin1 выполнить команду ipconfig для просмотра сетевых настроек. Убедиться, что скрипт управления успешно выполнился (IP-адрес изменен на 10.10.10.23).

A.11.4 СПО ПАС считается выдержавшим испытания по п. A.11.3.1-A.11.3.12 программы и методики испытаний и выполняющим пункты 3.2.1, 3.2.1.9 на СЧ ОКР, если:

- в едином графическом интерфейсе пользователь видит список контролируемых устройств:
  - сервер ServWin1;
  - сервер ServDeb1;
  - АРМ Оператора;
  - D-link DGS-1100-24.
- в едином графическом интерфейсе пользователь видит список скриптов, доступных для выбранного сетевого устройства (например, для сервера ServWin1):
  - показать версию ОС;
  - показать журнал Application;
  - показать журнал Security;
  - показать журнал System;
  - изменить IP адрес.

A.12 Методика № 12

A.12.1 В данной методике проводится проверка СПО ПАС на соответствие требованиям пунктов 3.2.1, 3.2.1.10 ТЗ на СЧ ОКР «Амезит-В».

A.12.2 В соответствии с требованиями пунктов 3.2.1, 3.2.1.10 ТЗ на СЧ ОКР «Амезит-В» СПО ПАС должно обеспечивать сетевую трансляцию адресов.

А.12.3 Для проведения проверки СПО ПАС на соответствие предъявляемым требованиям необходимо выполнить действия, описанные ниже.

А.12.3.1 Собрать испытательный стенд в соответствии со схемой на рисунке Рисунок 3.

А.12.3.2 Подключить АРМ оператора ПАС к испытательному стенду. Порядок подключения АРМ приведен в документе RU.ВАТС.00177-01 32 01 «Специальное программное обеспечение подсистемы формирования автономного сегмента сети передачи данных. Руководство системного программиста».

А.12.3.3 Выполнить команды, отображающие параметры сетевого соединения АРМ оператора ПАС; убедиться, что в испытательном стенде настроены и работают службы DHCP и DNS, а также что сетевому интерфейсу АРМ оператора ПАС назначен IP-адрес 10.10.10.12. Порядок настройки и просмотра сетевых параметров АРМ приведен в документе RU.ВАТС.00177-01 32 01 «Специальное программное обеспечение подсистемы формирования автономного сегмента сети передачи данных. Руководство системного программиста».

А.12.3.4 С АРМ оператора ПАС войти в консоль управления маршрутизатора D-link DGS-1100-24 и настроить правила трансляции (пул IP-адресов и набор разрешенных портов: 192.168.1.1 по 192.168.1.8 и 40200-42200). Инструкции по работе с маршрутизатором приведены в документе RU.ВАТС.00177-01 32 01 «Специальное программное обеспечение подсистемы формирования автономного сегмента сети передачи данных. Руководство системного программиста».

А.12.3.5 Загрузить обозреватель на АРМ оператора ПАС и выполнить запрос к информационному ресурсу, расположенному за пределами испытательного стенда (www.yandex.ru).

А.12.3.6 Выполнить вход в интерфейс оператора ПО мониторинга сетевого трафика, перейдя в раздел просмотра статистики соединений. Порядок просмотра статистики приведен в документе RU.ВАТС.00177-01 34 07 «Специальное программное обеспечение подсистемы формирования автономного сегмента сети передачи данных. Программное обеспечение мониторинга сетевого трафика. Руководство пользователя».

А.12.3.7 Найти соединение, поступившие с АРМ оператора ПАС (по IP-адресу10.10.10.12, который был выдан АРМ).

А.12.3.8 Просмотреть данные соединения. Убедиться, что при проходе сетевого пакета через маршрутизатор D-link DGS-1100-24 испытательного

стенда произошла трансляция сетевого IP-адреса (в исходящих пакетах изменился IP-адрес отравителя на 192.168.1.1).

А.12.4 СПО ПАС считается выдержавшим испытания по п. А.12.3.1-А.12.3.8 программы и методики испытаний и выполняющим пункты 3.2.1, 3.2.1.10 на СЧ ОКР, если обеспечивается сетевая трансляция адресов: сетевой адрес отправителя 10.10.10.12 был изменен на 192.168.1.1 при прохождении пакетом маршрутизатора D-link DGS-1100-24.

А.13 Методика № 13

А.13.1 В данной методике проводится проверка СПО ПАС на соответствие требованиям пунктов 3.2.1, 3.2.1.11 ТЗ на СЧ ОКР «Амезит-В».

А.13.2 В соответствии с требованиями пунктов 3.2.1, 3.2.1.11 ТЗ на СЧ ОКР «Амезит-В» СПО ПАС должно обеспечивать возможность устойчивого к несанкционированному доступу централизованного управления и мониторинга контролируемого оборудования с использованием единого графического интерфейса, обладающего возможностями:

- просмотра и редактирования списка контролируемого оборудования (устройство, набор контролируемых параметров);
- определения контролируемых параметров, ввода для контролируемых параметров диапазонов штатных значений;
- отображения текущих параметров оборудования в реальном времени (с заданной частотой обновления);
- определения событий, требующих оповещения оператора;
- удаленного обновления прошивки;
- просмотра диагностической информации.

Примечание. В роли контролируемых параметров могут выступать любые из стандартных параметров для контролируемого телекоммуникационного оборудования уровня ядра и уровня распределения.

А.13.3 Для проведения проверки СПО ПАС на соответствие предъявляемым требованиям необходимо выполнить действия, описанные ниже.

А.13.3.1 Собрать испытательный стенд в соответствии со схемой на рисунке Рисунок 3.

А.13.3.2 Выполнить вход в СПО ПАС, перейдя в раздел просмотра списка контролируемого оборудования (перечня технических средств, входящих в состав ПАС). Инструкции по работе с СПО ПАС приведены в документах RU.ВАТС.00177-01 34 05 «Специальное программное обеспечение подсистемы формирования автономного сегмента сети передачи данных.

Программное обеспечение диагностики и управления. Руководство системного программиста» и RU.BATC.00177-01 92 05 «Специальное программное обеспечение подсистемы формирования автономного сегмента сети передачи данных. Программное обеспечение диагностики и управления. Руководство пользователя».

А.13.3.3 Просмотреть записи, содержащие параметры контролируемого оборудования (технических средств). Убедиться, что пользователь имеет возможность централизованного мониторинга технических средств, входящих в состав испытательного стенда: контролируемое оборудование автономного сегмента сети отображается в виде списка (устройство, набор контролируемых параметров).

А.13.3.4 Добавить новое устройство (сервер ServWin1) в список контролируемых устройств, убедиться, что пользователь имеет возможность редактировать список контролируемого оборудования.

А.13.3.5 Выполнить настройки контролируемых параметров сервер ServWin1, а также задать граничные значения для CPU Load в 50%.

А.13.3.6 Определить события, требующие оповещения оператора (CPU Load больше 50%).

А.13.3.7 Убедиться, что пользователь СПО ПАС имеет возможность своевременного информирования и управления контролируемым оборудованием (техническими средствами) испытательного стенда: для этого для маршрутизатора D-link DGS-1100-24 добавить скрипт «Обновить версию прошивки».

А.13.4 СПО ПАС считается выдержавшим испытания по п. А.13.3.1-А.13.3.7 программы и методики испытаний и выполняющим пункты 3.2.1, 3.2.1.11 на СЧ ОКР, если:

- в списке контролируемых узлов появился сервер ServWin1;
- в списке графиков контролируемых параметров появился график CPU Load для сервера ServWin1;
- в списке скриптов для D-link DGS-1100-24 появился скрипт «Обновить версию прошивки».

А.14 Методика № 14

А.14.1 В данной методике проводится проверка СПО ПАС на соответствие требованиям пунктов 3.2.1, 3.2.1.12 ТЗ на СЧ ОКР «Амезит-В».

А.14.2 В соответствии с требованиями пунктов 3.2.1, 3.2.1.12 ТЗ на СЧ ОКР «Амезит-В» СПО ПАС должно обеспечивать сопряжение с каналообразующей аппаратурой различных опорных сетей передачи данных.

А.14.3 Для проведения проверки СПО ПАС на соответствие предъявляемым требованиям необходимо выполнить действия, описанные ниже.

А.14.3.1 Собрать испытательный стенд в соответствии со схемой на рисунке Рисунок 3.

А.14.3.2 Проверить наличие в составе ПАС оптических патч-кордов с типами коннекторов FC, SC, ST, LC; убедиться, что СПО формирования автономного сегмента сети передачи данных обеспечивает физическое сопряжение с каналообразующей аппаратурой различных опорных сетей передачи данных.

А.14.3.3 Проверить наличие в составе ПАС устройства для точной стыковки оптических волокон типа HU125, убедиться, что СПО формирования автономного сегмента сети передачи данных обеспечивает физическое сопряжение с каналообразующей аппаратурой различных опорных сетей передачи данных.

А.14.3.4 Проверить наличие в составе ПАС интерфейсов типа Ethernet и SFP, убедиться, что СПО формирования автономного сегмента сети передачи данных обеспечивает физическое сопряжение с каналообразующей аппаратурой различных опорных сетей передачи данных.

А.14.4 СПО ПАС считается выдержавшим испытания по п. А.14.3.1-А.14.3.4 программы и методики испытаний и выполняющим пункты 3.2.1, 3.2.1.12 на СЧ ОКР, если в составе СПО формирования автономного сегмента сети передачи данных присутствуют оптические патч-корды с типами коннекторов FC, SC, ST, LC; а также в составе СПО формирования автономного сегмента сети передачи данных присутствуют: устройство для точной стыковки оптических волокон типа HU125, интерфейсы типа Ethernet и SFP, которые обеспечивают физическое сопряжение ПАС с каналообразующей аппаратурой различных опорных сетей передачи данных.

А.15 Методика № 15

А.15.1 В данной методике проводится проверка СПО ПАС на соответствие требованиям пунктов 3.2.1, 3.2.1.13 ТЗ на СЧ ОКР «Амезит-В».

А.15.2 В соответствии с требованиями пунктов 3.2.1, 3.2.1.13 ТЗ на СЧ ОКР «Амезит-В» скорость передачи данных, поддерживаемая СПО ПАС, должна составлять:

- на уровне ядра (между коммутаторами уровня распределения и уровня ядра): не менее 10 Гбит/с при выполнении условия «нормальности» трафика, не менее 6 Гбит/с в противном случае;

- на уровне распределения (между коммутаторами уровня доступа и уровня распределения): не менее 1 Гбит/с при выполнении условия «нормальности» трафика, не менее 600 Мбит/с в противном случае;

- на уровне доступа (между пользователем и коммутатором уровня доступа): для проводных сетей связи – не менее 100 Мбит/с, для беспроводных сетей – не менее 80 Кбит/с.

Примечание. Здесь и далее под «нормальностью» трафика понимается трафик, в котором доля коротких пакетов (длиной до 64 байтов) не превышает 20%.

А.15.3 Для проведения проверки СПО ПАС на соответствие предъявляемым требованиям необходимо выполнить действия, описанные ниже.

А.15.3.1 Собрать испытательный стенд в соответствии со схемой на рисунке Рисунок 3.

А.15.3.2 Выполнить подключение генератора трафика (АПК СКАТ) к испытательному стенду. Порядок подключения генератора трафика (АПК СКАТ) и настройки испытательного стенда приведен в документе RU.ВАТС.00177-01 32 01 «Специальное программное обеспечение подсистемы формирования автономного сегмента сети передачи данных. Руководство системного программиста».

А.15.3.3 Выполнить вход в интерфейс настройки генератора трафика, установить параметры генерации трафика со скоростью 10 Гбит/с. Порядок запуска и настройки генератора трафика приведен в документе RU.ВАТС.00177-01 32 01 «Специальное программное обеспечение подсистемы формирования автономного сегмента сети передачи данных. Руководство системного программиста».

А.15.3.4 Выполнить вход в интерфейс оператора СПО ПАС, перейдя в раздел просмотра статистики. Порядок просмотра статистики приведен в документе RU.ВАТС.00177-01 34 07 «Специальное программное обеспечение подсистемы формирования автономного сегмента сети передачи данных. Программное обеспечение мониторинга сетевого трафика. Руководство пользователя».

А.15.3.5 Просмотреть статистику трафика, поступающего в СПО ПАС. Убедиться, что скорость передачи данных, поддерживаемая СПО на уровне ядра (между коммутаторами уровня распределения и уровня ядра), соответствует требованиям пункта 3.2.5.13 ТЗ (для физического интерфейса 10GBASE-LR) (при выполнении условия «нормальности» трафика (доля коротких пакетов (длиной до 64 байт) не превышает 20 %). Порядок просмотра

статистики приведен в документе RU.BATC.00177-01 34 07 «Специальное программное обеспечение подсистемы формирования автономного сегмента сети передачи данных. Программное обеспечение мониторинга сетевого трафика. Руководство пользователя».

А.15.4 СПО ПАС считается выдержавшим испытания по п. А.15.3.1-А.15.3.5 программы и методики испытаний и выполняющим пункты 3.2.1, 3.2.1.13 на СЧ ОКР, если СПО ПАС обеспечивает выполнение требований назначения по скорости передачи данных при выполнении условия «нормальности» трафика (доля коротких пакетов (длиной до 64 байт) не превышает 20 %), поддерживаемой СПО на уровне ядра (между коммутаторами уровня распределения и уровня ядра): скорость передачи данных должна составлять не менее 10 Гбит/с (для физического интерфейса 10GBASE-LR) (при выполнении условия «нормальности» трафика (доля коротких пакетов (длиной до 64 байт) не превышает 20 %).

А.15.4.1 Выполнить вход в интерфейс настройки генератора трафика, установить параметры генерации трафика со скоростью 6 Гбит/с (доля коротких пакетов (длиной до 64 байт) превышает 20 %).

А.15.4.2 Просмотреть статистику трафика, поступающего в СПО ПАС. Убедиться, что скорость передачи данных, поддерживаемая СПО на уровне ядра (между коммутаторами уровня распределения и уровня ядра), соответствует требованиям пункта 3.2.5.13 ТЗ (для физического интерфейса 10GBASE-LR) для трафика, не удовлетворяющего условию «нормальности».

А.15.5 СПО ПАС считается выдержавшим испытания по п. А.15.4.1-А.15.4.2 программы и методики испытаний и выполняющим пункты 3.2.1, 3.2.1.13 на СЧ ОКР, если СПО ПАС обеспечивает выполнение требований назначения по скорости передачи данных, поддерживаемой СПО на уровне распределения (между коммутаторами уровня доступа и уровня распределения при не выполнении условия «нормальности» трафика (доля коротких пакетов (длиной до 64 байт) превышает 20 %) скорость передачи данных должна составлять не менее 6 Гбит/с.

А.15.5.1 Выполнить вход в интерфейс настройки генератора трафика, установить параметры генерации трафика со скоростью 1 Гбит/с (для физических интерфейсов 1000DFSE-T, 1000BASE-SX).

А.15.5.2 Просмотреть статистику трафика, поступающего в СПО анализа трафика ПАС. Убедиться, что скорость передачи данных, поддерживаемая СПО на уровне распределения (между коммутаторами уровня доступа и уровня распределения), соответствует требованиям пункта 3.2.5.13

ТЗ для физических интерфейсов 1000DFSE-T или 1000BASE-SX должна составлять не менее 1 Гбит/с.

А.15.5.3 Выполнить вход в интерфейс настройки генератора трафика, установить параметры генерации трафика, не удовлетворяющего условию «нормальности» со скоростью 600 Мбит/с (для физических интерфейсов 1000DFSE-T, 1000BASE-SX).

А.15.6 СПО ПАС считается выдержавшим испытания по п. А.15.5.1-А.15.5.3 программы и методики испытаний и выполняющим пункты 3.2.1, 3.2.1.13 на СЧ ОКР, если СПО ПАС обеспечивает выполнение требований назначения по скорости передачи данных, поддерживаемой СПО на уровне распределения (между коммутаторами уровня доступа и уровня распределения при не выполнении условия «нормальности» трафика (доля коротких пакетов длиной до 64 байт превышает 20 %) скорость передачи данных составляет не менее 600 Мбит/с.

А.15.6.1 Выполнить вход в интерфейс настройки генератора трафика, установить параметры генерации трафика со скоростью 100 Мбит/с для физического интерфейса 100BASE-FX.

А.15.6.2 Просмотреть статистику трафика, поступающего в СПО ПАС. Убедиться, что скорость передачи данных, поддерживаемая СПО на уровне доступа (между пользователем и коммутатором уровня доступа), для проводных сетей связи соответствует требованиям пункта 3.2.5.13 ТЗ (для физического интерфейса 100BASE-FX).

А.15.7 СПО ПАС считается выдержавшим испытания по п. А.15.6.1-А.15.6.2 программы и методики испытаний и выполняющим пункты 3.2.1, 3.2.1.13 на СЧ ОКР, если СПО ПАС обеспечивает выполнение требований назначения по скорости передачи данных при выполнении условия «нормальности» трафика (доля коротких пакетов (длиной до 64 байт) не превышает 20 %), на уровне доступа скорость передачи данных составляет не менее 100 Мбит/с.

А.15.7.1 Выполнить вход в интерфейс настройки генератора трафика, установить параметры генерации трафика со скоростью 80 Кбит/с (для моделирования трафика, поступающего по беспроводным линиям связи).

А.15.7.2 Просмотреть статистику трафика, поступающего в СПО ПАС. Убедиться, что скорость передачи данных для беспроводной сети соответствует требованиям пункта 3.2.5.13 ТЗ.

А.15.7.3 СПО ПАС считается выдержавшим испытания по п. А.15.7.1-А.15.7.3 программы и методики испытаний и выполняющим пункты 3.2.1, 3.2.1.13 на СЧ ОКР, если СПО ПАС обеспечивает выполнение требований

назначения по скорости передачи данных беспроводных сетей не менее 80 Кбит/с.

А.16 Методика № 16

А.16.1 В данной методике проводится проверка СПО ПАС на соответствие требованиям пунктов 3.2.1, 3.2.1.14 ТЗ на СЧ ОКР «Амезит-В».

А.16.2 В соответствии с требованиями пунктов 3.2.1, 3.2.1.14 ТЗ на СЧ ОКР «Амезит-В» СПО ПАС должно обеспечивать контроль состояния телекоммуникационного оборудования, оперативного выявления попыток получения НСД к ним, нештатных перезагрузок ОС аппаратного обеспечения и иных фактов нарушения ИБ подсистемы ПАС, в том числе:

- несанкционированный доступ с правами суперпользователя;
- установка дополнительного (вредоносного) ПО;
- реализация атак типа «отказ в обслуживании».

Перечень действий, относящихся к нарушению ИБ контролируемого оборудования, также включает в себя следующие события:

- неудачные попытки аутентификации на устройстве;
- появление нештатных учетных записей;
- выполнение входа на устройство в необычное время;
- выполнение входа на устройство с нештатного сетевого узла;
- перезагрузка устройства;
- изменение конфигурации устройства;
- изменение контрольных сумм конфигурационных и системных файлов;
- события, свидетельствующие о сбоях ПО;
- снижение производительности устройства ниже штатных значений;
- рост объема сетевого трафика на портах оборудования выше штатных значений;
- срабатывание встроенных защитных механизмов канального уровня (в том числе, port security, dynamic ARP inspection, IP source guard);
- увеличение времени отклика устройства;
- потеря связи с устройством.

Примечание. Контроль состояния телекоммуникационного оборудования должен осуществляться при помощи единого графического интерфейса, отображающего сообщения о выявлении фактов нарушения ИБ и поддерживающего оповещение администратора АПК.

А.16.3 Для проведения проверки СПО ПАС на соответствие предъявляемым требованиям необходимо выполнить действия, описанные ниже.

А.16.3.1 Собрать испытательный стенд в соответствии со схемой на рисунке Рисунок 3.

А.16.3.2 С АРМ оператора ПАС выполнить попытку входа от имени администратора на маршрутизатор D-link DGS-1100-24.

А.16.3.3 СПО ПАС считается выдержавшим испытания по п. А.16.3.1-А.16.3.2 программы и методики испытаний и выполняющим пункты 3.2.1, 3.2.1.14 на СЧ ОКР, если пользователь может видеть сообщения о событии входа вида:

14:59:46 Предупреждение 15:00:15 ServWin1 Совершен вход в систему

А.16.3.4 На сервере ServWin1 выполнить вход в консоль управления под пользователем «Администратор» и создать учетную запись User10.

А.16.3.5 СПО ПАС считается выдержавшим испытания по п. А.16.3.4 программы и методики испытаний и выполняющим пункты 3.2.1, 3.2.1.14 на СЧ ОКР, если пользователь может видеть сообщение о создании учетных записей вида:

14:59:46 Предупреждение 15:00:15 ServWin1 Создана учетная запись для User10

А.16.3.6 С АРМ оператора войти в СПО ПАС и для сервера ServWin1 установить штаное время работы с 16-00 по 23-00.

А.16.3.7 С АРМ оператора ПАС выполнить попытку входа на сервер ServWin1 под правами администратора в нештатное время (14-59).

А.16.3.8 СПО ПАС считается выдержавшим испытания по п. А.16.3.6-А.16.3.7 программы и методики испытаний и выполняющим пункты 3.2.1, 3.2.1.14 на СЧ ОКР, если пользователь может видеть сообщение о попытке входа в нештатное время:

14:59:46 Предупреждение 15:00:15 ServWin1 Совершен вход в систему в нештатное время

А.16.3.9 С АРМ оператора войти в СПО ПАС и для сервера ServWin1 установить штатный IP адрес для входа 10.10.01.32.

А.16.3.10 С АРМ оператора ПАС выполнить попытку административного входа на сервер ServWin1 с АРМ оператора с адресом 10.10.01.10.

А.16.3.11 СПО ПАС считается выдержавшим испытания по п. А.16.3.9-А.16.3.10 программы и методики испытаний и выполняющим пункты 3.2.1,

3.2.1.14 на СЧ ОКР, если пользователь может видеть сообщение о попытке входа с нештатного сетевого узла:

14:59:46 Предупреждение 15:00:15 ServWin1 Совершен вход в систему с нештатного узла

А.16.3.12 С АРМ оператора ПАС выполнить перезагрузку сервера ServWin1.

А.16.3.13 СПО ПАС считается выдержавшим испытания по п. А.16.3.12 программы и методики испытаний и выполняющим пункты 3.2.1, 3.2.1.14 на СЧ ОКР, если пользователь может видеть сообщение о перезагрузке:

4:56:10 Предупреждение 14:56:40 ServWin1 has just been restarted

А.16.3.14 С АРМ оператора ПАС войти в ПО управления D-link DGS-1100-24 (войти в консоль управления) и изменить конфигурацию: отключить порт 14.

А.16.3.15 СПО ПАС считается выдержавшим испытания по п. А.16.3.14 программы и методики испытаний и выполняющим пункты 3.2.1, 3.2.1.14 на СЧ ОКР, если пользователь может видеть сообщение об изменении конфигурации:

15:49:46 Предупреждение 15:50:15 D-link DGS-1100-24 Изменена конфигурация сетевого устройства

А.16.3.16 С АРМ оператора войти в СПО ПАС и для сервера ServWin1 установить проверку контрольных сумм для файла c:/system.

А.16.3.17 С АРМ оператора ПАС войти на сервер ServWin1 и выполнить изменение файла c:/system.

А.16.3.18 СПО ПАС считается выдержавшим испытания по п. А.16.3.16-А.16.3.17 программы и методики испытаний и выполняющим пункты 3.2.1, 3.2.1.14 на СЧ ОКР, если пользователь может видеть сообщение об изменении контрольных сумм файлов:

10:16:10 Предупреждение 10:20:40 ServWin1 Изменилась контрольная сумма c:/system

А.16.3.19 С АРМ оператора ПАС войти на сервер ServWin1 и запустить программу fault.exe (моделируется событие сбоя ПО).

А.16.3.20 СПО ПАС считается выдержавшим испытания по п. А.16.3.19 программы и методики испытаний и выполняющим пункты 3.2.1, 3.2.1.14 на СЧ ОКР, если пользователь может видеть сообщение о сбое ПО:

14:59:46 Предупреждение 15:00:15 ServWin1 Сбой ПО

А.16.3.21 С АРМ оператора ПАС войти на сервер ServWin1 и запустить программу burnn.exe (моделируется высокая загрузка).

А.16.3.22 СПО ПАС считается выдержавшим испытания по п. А.16.3.21 программы и методики испытаний и выполняющим пункты 3.2.1, 3.2.1.14 на СЧ ОКР, если пользователь может видеть сообщение о высокой загрузке процессора:

14:59:46 Предупреждение 15:00:15 ServWin1 CPULoad is too high

А.16.3.23 Смоделировать рост объема сетевого трафика на портах D-link DGS-1100-24.

А.16.3.24 СПО ПАС считается выдержавшим испытания по п. А.16.3.23 программы и методики испытаний и выполняющим пункты 3.2.1, 3.2.1.14 на СЧ ОКР, если пользователь может видеть сообщение:

14:59:46 Предупреждение 15:00:15 D-link DGS-1100-24 Traffic is too high

А.16.3.25 Смоделировать срабатывание встроенных защитных механизмов канального уровня (port security, dynamic ARP inspection, IP source guard) Dlink DGS-3120, путем подключения к порту коммутатора 10 АРМ оператора ПАС.

А.16.3.26 СПО ПАС считается выдержавшим испытания по п. А.16.3.25 программы и методики испытаний и выполняющим пункты 3.2.1, 3.2.1.14 на СЧ ОКР, если пользователь может видеть сообщения о создании учетных записей вида:

14:59:46 Предупреждение 15:00:15 D-link DGS-1100-24 Событие port security 10

А.16.3.27 С АРМ оператора ПАС войти на консоль маршрутизатора D-link DGS-1100-24 и дать команду на выключение.

А.16.3.28 СПО ПАС считается выдержавшим испытания по п. А.16.3.27 программы и методики испытаний и выполняющим пункты 3.2.1, 3.2.1.14 на СЧ ОКР, если пользователь может видеть сообщение о недоступности маршрутизатора:

14:59:46 Предупреждение 15:00:15 D-link DGS-1100-24 Response time is too high on D-link DGS-1100-24 29с Нет

А.17 Методика № 17

А.17.1 В данной методике проводится проверка СПО ПКС на соответствие требованиям пунктов 3.2.2, 3.2.2.1 ТЗ на СЧ ОКР «Амезит-В».

А.17.2 В соответствии с требованиями пунктов 3.2.2, 3.2.2.1 ТЗ на СЧ ОКР «Амезит-В» СПО ПКС должно обеспечивать анализ соединений автономного сегмента сети передачи данных и сбор информации на скорости до 6 Гбит/с.

Примечание: анализ и сбор информации должен выполняться на прикладном уровне модели OS1.

А.17.3 Для проведения проверки СПО ПКС на соответствие предъявляемым требованиям необходимо выполнить действия, описанные ниже.

А.17.3.1 Собрать испытательный стенд в соответствии со схемой (см. рисунок Рисунок 4).

А.17.3.2 Выполнить подключение генератора трафика (АПК СКАТ) к испытательному стенду. Порядок подключения генератора трафика (АПК СКАТ) и настройки испытательного стенда приведен в документе RU.BATC.00178-01 32 01 «Специальное программное обеспечение подсистемы контроля сообщений автономного сегмента сети передачи данных. Руководство системного программиста».

А.17.3.3 Выполнить запуск генератора трафика, который обеспечивает устойчивый трафик по протоколу прикладного уровня модели OSI со скоростью 6 Гбит/с, проходящий через ПО мониторинга сетевого трафика ПКС (в трафике передается файл mail010). Порядок запуска и настройки генератора трафика приведен в документе RU.BATC.00178-01 34 01 «Специальное программное обеспечение подсистемы контроля сообщений автономного сегмента сети передачи данных. Руководство оператора».

А.17.3.4 Выполнить вход в интерфейс оператора ПО мониторинга сетевого трафика ПКС, перейти в раздел просмотра статистики соединений. Описание интерфейса ПО мониторинга сетевого трафика ПКС представлено в документе RU.BATC.00178-01 34 01 «Специальное программное обеспечение подсистемы контроля сообщений автономного сегмента сети передачи данных. Руководство оператора».

А.17.3.5 Выполнить вход в консоль управления ПКС. Инструкции по работе приведены в документе RU.BATC.00178-01 32-01 «Специальное

программное обеспечение подсистемы контроля сообщений автономного сегмента сети передачи данных. Руководство системного программиста».

А.17.3.6 Просмотреть статистику трафика, проходящего через ПКС. Убедиться, что выполняется анализ соединений сегмента сети передачи данных и сбор информации о них. Порядок просмотра статистики приведен в RU.BATC.00178-01 32 01 «Специальное программное обеспечение подсистемы контроля сообщений автономного сегмента сети передачи данных. Руководство системного программиста».

А.17.4 СПО ПКС считается выдержавшим испытания по п. А.17.3.1-А.17.3.6 программы и методики испытаний и выполняющим пункты 3.2.2, 3.2.2.1 ТЗ на СЧ ОКР, если:

- выполняется сбор информации на скорости до 6 Гбит/с;
- выполняется анализ собранной информации (разборка протоколов и сохранение передаваемых сообщений)(в выходной директории появился файл mail010).

А.18 Методика № 18

А.18.1 В данной методике проводится проверка СПО ПКС на соответствие требованиям пунктов 3.2.2, 3.2.2.2 ТЗ на СЧ ОКР «Амезит-В».

А.18.2 В соответствии с требованиями пунктов 3.2.2, 3.2.2.2 ТЗ на СЧ ОКР «Амезит-В» СПО ПКС должно обеспечивать организацию узлов промежуточного контроля с целью анализа соединений и выявления информации при использовании протоколов типа IPSEC.

А.18.3 Для проведения проверки СПО ПКС на соответствие предъявляемым требованиям необходимо выполнить действия, описанные ниже.

А.18.3.1 Собрать испытательный стенд в соответствии со схемой (см. рисунок Рисунок 4).

А.18.3.2 Выполнить подключение генератора трафика (АПК СКАТ) к испытательному стенду. Порядок подключения генератора трафика (АПК СКАТ) и настройки испытательного стенда приведен в документе RU.BATC.00178-01 32 01 «Специальное программное обеспечение подсистемы контроля сообщений автономного сегмента сети передачи данных. Руководство системного программиста».

А.18.3.3 Выполнить подключение узла промежуточного контроля (сервера хранения трафика ПКС), на котором установлено ПО мониторинга сетевого трафика ПКС, к испытательному стенду.

А.18.3.4 Выполнить настройку ПО мониторинга сетевого трафика ПКС, обеспечивающую извлечение и сохранение парольно-адресной информации (извлечение выполняется путем проведения атаки MITM). Порядок настройки ПО мониторинга сетевого трафика ПКС представлен в документе RU.BATC.00178-01 32 01 «Специальное программное обеспечение подсистемы контроля сообщений автономного сегмента сети передачи данных. Руководство системного программиста».

А.18.3.5 Выполнить запуск генератора трафика (АПК СКАТ), который обеспечивает устойчивый трафик (трафик моделирует вход на ресурс с парольно-адресной информацией: «user100» и «password100») по протоколу IPSEC, проходящий через ПО мониторинга сетевого трафика ПКС. Инструкции по работе с генератором трафика представлены в документе RU.BATC.00178-01 34 01 «Специальное программное обеспечение подсистемы контроля сообщений автономного сегмента сети передачи данных. Руководство оператора».

А.18.3.6 Выполнить вход в ПО мониторинга сетевого трафика, работающее на промежуточном узле, и перейти в директорию, содержащую извлеченную парольно-адресную информацию. Инструкции по работе с ПО мониторинга сетевого трафика представлены в документе RU.BATC.00178-01 34 01 «Специальное программное обеспечение подсистемы контроля сообщений автономного сегмента сети передачи данных. Руководство оператора».

А.18.3.7 Выполнить просмотр файлов, содержащих парольно-адресную информацию. Убедиться, что организовано прохождение трафика через узел промежуточного контроля, которое обеспечивает получение доступа к информации, передаваемой с использованием протоколов типа IPSEC.

А.18.4 СПО ПКС считается выдержавшим испытания по п. А.18.3.1-А.18.3.7 программы и методики испытаний и выполняющим пункты 3.2.2, 3.2.2.2 ТЗ на СЧ ОКР, если оператор путем организации узла промежуточного контроля (сервер хранения трафика ПКС) извлекает парольно-адресную информацию: «user100» и «password100».

А.19 Методика № 19

А.19.1 В данной методике проводится проверка СПО ПКС на соответствие требованиям пунктов 3.2.2, 3.2.2.3 ТЗ на СЧ ОКР «Амезит-В».

А.19.2 В соответствии с требованиями пунктов 3.2.2, 3.2.2.3 ТЗ на СЧ ОКР «Амезит-В» СПО ПКС должно обеспечивать автоматическое распознавание и отбор файлов.

Примечания:

1. Перечень типов файлов, подлежащих распознаванию и отбору: HTML, GIF, JPEG, PNG, PDF, AVI, MPEG, DOC (DOCX), XLS (XLSX), PPT (PPTX), PPS, ZIP, GZIP, ARJ, RAR, BZIP, MP3, WAV, BMP, CDR, RTF, CSV, MPP, PST, XHTML, MHT, SXW, SXC, SXI, SXD, SXM, ODS, ODP, ODG, ODF, MDF, DBF, DB, MYD, DBQUERY, VSD

2. Перечень протоколов, подлежащих распознаванию и анализу: FTP, HTTP, POP/POP3, IMAP, SMTP, TELNET.

3. Должны быть предусмотрены меры по предотвращению использования криптографически защищенных версий указанных протоколов.

4. При обработке почтовых сообщений должна быть извлечена и зарегистрирована следующая информация:

- дата и время передачи почтового сообщения;
- отправитель почтового сообщения;
- список получателей почтового сообщения;
- список получателей копии почтового сообщения;
- содержимое почтового сообщения.

А.19.3 Для проведения проверки СПО ПКС на соответствие предъявляемым требованиям необходимо выполнить действия, описанные ниже.

А.19.3.1 Собрать испытательный стенд в соответствии со схемой (см. рисунок Рисунок 4).

А.19.3.2 Выполнить подключение генератора трафика (АПК СКАТ) к испытательному стенду. Порядок подключения генератора трафика (АПК СКАТ) и настройки испытательного стенда приведен в документе RU.ВАТС.00178-01 32 01 «Специальное программное обеспечение подсистемы контроля сообщений автономного сегмента сети передачи данных. Руководство системного программиста».

А.19.3.3 Выполнить вход в интерфейс оператора ПО мониторинга сетевого трафика ПКС, перейдя в раздел настройки форматов распознаваемых файлов, и ввести правила распознавания и сохранения извлеченных файлов. Описание интерфейса ПО мониторинга сетевого трафика ПКС представлено в документе RU.ВАТС.00178-01 34 01 «Специальное программное обеспечение подсистемы контроля сообщений автономного сегмента сети передачи данных. Руководство оператора».

А.19.3.4 Выполнить ввод правил распознавания файлов. Перечень типов распознаваемых файлов приведен в документе RU.ВАТС.00178-01 32 01 «Специальное программное обеспечение подсистемы контроля сообщений

автономного сегмента сети передачи данных. Руководство системного программиста».

А.19.3.5 Выполнить запуск генератора трафика, обеспечивающий передачу файлов (перечень типов файлов, подлежащих распознаванию и отбору: HTML, GIF, JPEG, PNG, PDF, AVI, MPEG, DOC (DOCX), XLS (XLSX), PPT (PPTX), PPS, ZIP, GZIP, ARJ, RAR, BZIP, MP3, WAV, BMP, CDR, RTF, CSV, MPP, PST, XHTML, MHT, SXW, SXC, SXI, SXD, SXM, ODS, ODP, ODG, ODF, MDF, DBF, DB, MYD, DBQUERY, VSD, путем использования протоколов: FTP, HTTP, POP/POP3, IMAP, SMTP, TELNET. Инструкции по работе с генератором трафика представлены в документе RU.BATC.00178-01 32 01 «Специальное программное обеспечение подсистемы контроля сообщений автономного сегмента сети передачи данных. Руководство системного программиста».

А.19.3.6 Перейти в директорию, в которую помещаются результаты извлечения файлов из трафика. Описание СПО ПКС представлено в документе RU.BATC.00178-01 34 01 «Специальное программное обеспечение подсистемы контроля сообщений автономного сегмента сети передачи данных. Руководство оператора».

А.19.3.7 Выполнить просмотр и сравнение размеров, контрольных сумм исходных файлов в директории генератора трафика и файлов в директории, в которую помещаются результаты извлечения файлов из трафика. Убедиться, что в соответствии с перечнем распознаваемых протоколов: FTP, HTTP, POP/POP3, IMAP, SMTP, SNMP, SPDY, TELNET из трафика извлечены и сохранены файлы. Перечень форматов файлов приведен в документе RU.BATC.00178-01 32 01 «Специальное программное обеспечение подсистемы контроля сообщений автономного сегмента сети передачи данных. Руководство системного программиста».

А.19.3.8 Выполнить вход в интерфейс оператора ПО мониторинга сетевого трафика ПКС, перейдя в раздел настройки сохранения статистики почтовых сообщений. Описание интерфейса ПО мониторинга сетевого трафика ПКС представлено в документе RU.BATC.00178-01 34 01 «Специальное программное обеспечение подсистемы контроля сообщений автономного сегмента сети передачи данных. Руководство оператора».

А.19.3.9 Выполнить ввод параметров сохранения статистики почтовых сообщений. Описание интерфейса ПО мониторинга сетевого трафика ПКС представлено в документе RU.BATC.00178-01 34 01 «Специальное программное обеспечение подсистемы контроля сообщений автономного сегмента сети передачи данных. Руководство оператора».

А.19.3.10 Выполнить запуск генератора трафика, который обеспечивает моделирование трафика обмена почтовыми сообщениями (файл mail010). Инструкции по работе с генератором трафика представлены в документе RU.BATC.00178-01 32 01 «Специальное программное обеспечение подсистемы контроля сообщений автономного сегмента сети передачи данных. Руководство системного программиста».

А.19.3.11 Перейти в директорию, содержащую извлеченные почтовые сообщения, и проверить наличие файла с извлеченными почтовыми сообщениями. Описание СПО ПКС представлено в документе RU.BATC.00178-01 34 01 «Специальное программное обеспечение подсистемы контроля сообщений автономного сегмента сети передачи данных. Руководство оператора».

А.19.3.12 Убедиться, что в соответствии с параметрами сохранения статистики почтовых сообщений автоматически извлечена и зарегистрирована следующая информация: дата и время передачи почтового сообщения, отправитель почтового сообщения, список получателей почтового сообщения, включая получателей копии почтового сообщения, при этом содержимое почтового сообщения сохранено на диске. Описание статистики почтовых сообщений представлено в документе RU.BATC.00178-01 34 01 «Специальное программное обеспечение подсистемы контроля сообщений автономного сегмента сети передачи данных. Руководство оператора».

А.19.4 СПО ПКС считается выдержавшим испытания по п. А.19.3.1-А.19.3.12 программы и методики испытаний и выполняющим пункты 3.2.2, 3.2.2.3 ТЗ на СЧ ОКР, если:

- есть возможность настраивать перечень распознаваемых форматов файлов и протоколов (HTML, GIF, JPEG, PNG, PDF, AVI, MPEG, DOC (DOCX), XLS (XLSX), PPT (PPTX), PPS, ZIP, GZIP, ARJ, RAR, BZIP, MP3, WAV, BMP, CDR, RTF, CSV, MPP, PST, XHTML, MHT, SXW, SXC, SXI, SXD, SXM, ODS, ODP, ODG, ODF, MDF, DBF, DB, MYD, DBQUERY, VSD)(протоколов: FTP, HTTP, POP/POP3, IMAP, SMTP, TELNET);
- при перехвате трафика выполняется автоматическое распознавание и извлечение файлов в соответствии с указанным перечнем форматов файлов и протоколов;
- выполняется регистрация статистики почтовых сообщений и автоматическое извлечение содержимого почтовых сообщений, которые сохраняются на жесткий диск в виде файла mail010.

А.20 Методика № 20

А.20.1 В данной методике проводится проверка СПО ПКС на соответствие требованиям пунктов 3.2.2, 3.2.2.4 ТЗ на СЧ ОКР «Амезит-В».

А.20.2 В соответствии с требованиями пунктов 3.2.2, 3.2.2.4 ТЗ на СЧ ОКР «Амезит-В» СПО ПКС должно обеспечивать предотвращение использования технологий анонимизации пользователей, в том числе:

- блокирование сетевых соединений к сервисам-анонимайзерам на основе URL-фильтрации;
- блокирование сетевых соединений к прокси-серверам на основе фильтрации сетевых адресов;
- блокирование сетевых соединений к IP-адресам узлов, ассоциированных с сетями анонимизации Tor и I2P, выявленных на основе фильтрации сетевых адресов;
- блокирование соединений на транспортные порты, ассоциированные с распространенными HTTP-прокси-серверами;
- блокирование доступа к VPN-сервисам по спискам IP-адресов/URL;
- блокирование соединений на транспортные порты, ассоциированные с VPN-сервисами;
- блокирование широко разрекламированных (основных) ресурсов, с которых ведется распространение инструментальных средств для организации анонимных сеансов (таких, как Tor Browser).

Примечание. Головным исполнителем должны быть сформированы первоначальные списки фильтрации и разработаны программные средства для поддержания их в актуальном состоянии.

А.20.3 Для проведения проверки СПО ПКС на соответствие предъявляемым требованиям необходимо выполнить действия, описанные ниже.

А.20.3.1 Собрать испытательный стенд в соответствии со схемой (см. рисунок Рисунок 4).

А.20.3.2 Выполнить подключение генератора трафика (АПК СКАТ) к испытательному стенду. Порядок подключения генератора трафика (АПК СКАТ) и настройки испытательного стенда приведен в документе RU.BATC.00178-01 32 01 «Специальное программное обеспечение подсистемы контроля сообщений автономного сегмента сети передачи данных. Руководство системного программиста».

А.20.3.3 Выполнить вход в интерфейс оператора ПО мониторинга сетевого трафика ПКС, перейдя в раздел настройки правил блокировки протоколов. Выполнить ввод правил блокировки протоколов. Описание

интерфейса ПО мониторинга сетевого трафика ПКС, а также действия по его настройке приведены в документах: RU.BATC.00178-01 32 01 «Специальное программное обеспечение подсистемы контроля сообщений автономного сегмента сети передачи данных. Руководство системного программиста», RU.BATC.00178-01 34 01 «Специальное программное обеспечение подсистемы контроля сообщений автономного сегмента сети передачи данных. Руководство оператора».

А.20.3.4 Выполнить настройку автоматического обновления списка правил блокировки. Описание настройки автоматического обновления списка правил приведено в документе RU.BATC.00178-01 32 01 «Специальное программное обеспечение подсистемы контроля сообщений автономного сегмента сети передачи данных. Руководство системного программиста».

А.20.3.5 Выполнить запуск генератора трафика (АПК СКАТ), который обеспечивает трафик, содержащий:

- сетевые соединения к сервисам-анонимайзерам;
- сетевые соединения к прокси-серверам (10.10.10.21);
- сетевые соединения к IP-адресам узлов, ассоциированным с сетями анонимизации Tor и I2P (на примере www.torproject.org);
- соединения на транспортные порты, ассоциированные с распространенными HTTP-прокси-серверами (2775, 32142).

Инструкции по работе с генератором трафика приведены в документе RU.BATC.00178-01 32 01«Специальное программное обеспечение подсистемы контроля сообщений автономного сегмента сети передачи данных. Руководство системного программиста».

А.20.3.6 Выполнить вход в интерфейс оператора ПО мониторинга сетевого трафика ПКС, перейдя в раздел просмотра статистики соединений. Описание интерфейса ПО мониторинга сетевого трафика ПКС приведено в документе RU.BATC.00178-01 34 01 «Специальное программное обеспечение подсистемы контроля сообщений автономного сегмента сети передачи данных. Руководство оператора».

А.20.3.7 Выполнить просмотр статистики соединений. Убедиться, что трафик перечисленных выше протоколов, используемых технологиями анонимизации, блокирован (в статистике отсутствуют соединения по перечисленным выше протоколам).

А.20.3.8 Выполнить вход в интерфейс генератора трафика для просмотра журнала работы генератора трафика. Инструкции по работе с генератором трафика приведены в документе RU.BATC.00178-01 32 01 «Специальное программное обеспечение подсистемы контроля сообщений

автономного сегмента сети передачи данных. Руководство системного программиста».

А.20.3.9 Выполнить просмотр журнала работы генератора трафика. Убедиться, что все попытки организовать соединения по протоколам анонимизации были неуспешны.

А.20.4 СПО ПКС считается выдержавшим испытания по п. А.20.3.1-А.20.3.9 программы и методики испытаний и выполняющим пункты 3.2.2, 3.2.2.4 ТЗ на СЧ ОКР, если ПО мониторинга сетевого трафика ПКС выполняет автоматическую блокировку соединений:

- к прокси-серверу (при этом блокируемые ресурсы указаны в виде списка IP-адресов);
- к ресурсу www.torproject.org (при этом блокируемые ресурсы указаны в виде списка URL);
- на транспортные порты 2775, 32142 (при этом номера транспортных портов указаны в виде списка).

А.21 Методика № 21

А.21.1 В данной методике проводится проверка СПО ПКС на соответствие требованиям пунктов 3.2.2, 3.2.2.5 ТЗ на СЧ ОКР «Амезит-В».

А.21.2 В соответствии с требованиями пунктов 3.2.2, 3.2.2.5 ТЗ на СЧ ОКР «Амезит-В» СПО ПКС должно обеспечивать блокировку и перенаправление клиентских запросов (HTTP/HTTPS) на легитимные ресурсы ГИС ОП (зеркала).

П р и м е ч а н и я :

1. Блокируемые ресурсы задаются в виде списка URL (содержащего hostname или IP).
2. Для каждого из блокируемых ресурсов должна быть реализована возможность указать IP адрес веб-сервера, на который следует перенаправить поступающий запрос.
3. Должна быть предусмотрена возможность организаций нескольких зеркал (с различным наполнением) на одном IP.

А.21.3 Для проведения проверки СПО ПКС на соответствие предъявляемым требованиям необходимо выполнить действия, описанные ниже.

А.21.3.1 Собрать испытательный стенд в соответствии со схемой (см. Рисунок 4).

А.21.3.2 Перед началом проверки подготовить сайты-дубликаты одного легитимного ресурса news000.ru (не менее двух различных копий: news100.ru и news200.ru). Подготовка сайта-дубликата приведена в документах:

RU.ВАТС.00178-01 32 01 «Специальное программное обеспечение подсистемы контроля сообщений автономного сегмента сети передачи данных. Руководство системного программиста», RU.ВАТС.00178-01 34 01 «Специальное программное обеспечение подсистемы контроля сообщений автономного сегмента сети передачи данных. Руководство оператора».

А.21.3.3 Выполнить вход в интерфейс оператора ПО мониторинга сетевого трафика ПКС, перейдя в раздел настройки IP-адресов – «двойников» ресурсов глобальной информационной системы общего пользования (ГИС ОП). Описание интерфейса ПО мониторинга сетевого трафика ПКС приведено в документе RU.ВАТС.00178-01 34 01 01 «Специальное программное обеспечение подсистемы контроля сообщений автономного сегмента сети передачи данных. Руководство оператора». Настроить правила перенаправления с news000.ru на news100.ru.

А.21.3.4 В интерфейсе оператора ПО мониторинга сетевого трафика ПКС задать перечень IP-адресов или имен хостов, определяющих список ресурсов, запросы к которым (по протоколам HTTP\HTTPS) должны быть перенаправлены. В качестве ресурса-«двойника» указать IP-адрес первого сайта-дубликата. Описание интерфейса ПО мониторинга сетевого трафика ПКС приведено в документе RU.ВАТС.00178-01 34 01 «Специальное программное обеспечение подсистемы контроля сообщений автономного сегмента сети передачи данных. Руководство оператора».

А.21.3.5 Подключить АРМ оператора к сети сегмента. Описание подключения приведено в документе RU.ВАТС.00178-01 32 01 «Специальное программное обеспечение подсистемы контроля сообщений автономного сегмента сети передачи данных. Руководство системного программиста».

А.21.3.6 На АРМ оператора выполнить просмотр веб-страницы легитимного ресурса. Убедиться, что было выполнено перенаправление запроса на первый сайт-дубликат.

А.21.3.7 Выполнить вход в интерфейс оператора ПО мониторинга сетевого трафика ПКС, перейдя в раздел настройки IP-адресов – «двойников» ресурсов. Выполнить настройку переключения легитимного ресурса на второй сайт-дубликат. Описание интерфейса ПО мониторинга сетевого трафика ПКС приведено в документе RU.ВАТС.00178-01 34 01 01 «Специальное программное обеспечение подсистемы контроля сообщений автономного сегмента сети передачи данных. Руководство пользователя».

А.21.3.8 На АРМ оператора выполнить просмотр веб-страницы легитимного ресурса. Убедиться, что было выполнено перенаправление запроса на второй сайт-дубликат.

А.21.4 СПО ПКС считается выдержавшим испытания по п. А.21.3.1-А.21.3.8 программы и методики испытаний и выполняющим пункты 3.2.2, 3.2.2.5 ТЗ на СЧ ОКР, если:

- обеспечивается перенаправление клиентских запросов на легитимные ресурсы ГИС ОП (с сайта news000.ru на сайт news100.ru);
- в интерфейсе есть возможность настройки перечня легитимных ресурсов ГИС ОП (news000.ru), запрос к которым должен быть перенаправлен на сайт-дубликат, при этом ПО мониторинга сетевого трафика ПКС обеспечивает возможность хранения нескольких сайтов-дубликатов легитимного ресурса (news100.ru, news200.ru).

А.22 Методика № 22

А.22.1 В данной методике проводится проверка СПО ПКС на соответствие требованиям пунктов 3.2.2, 3.2.2.6 ТЗ на СЧ ОКР «Амезит-В».

А.22.2 В соответствии с требованиями пунктов 3.2.2, 3.2.2.6 ТЗ на СЧ ОКР «Амезит-В» СПО ПКС должно обеспечивать возможность выбора заданного абонента путем задания оператором совокупности коммутационно-адресных признаков, в том числе IP-адреса, IP-маски, МАС-адреса, адреса протоколов прикладного уровня.

А.22.3 Для проведения проверки СПО ПКС на соответствие предъявляемым требованиям необходимо выполнить действия, описанные ниже.

А.22.3.1 Собрать испытательный стенд в соответствии со схемой (см. Рисунок 4).

А.22.3.2 Выполнить вход в интерфейс оператора ПО мониторинга сетевого трафика ПКС, перейти в раздел ввода правил отбора материалов информационного обмена абонента. Описание интерфейса ПО мониторинга сетевого трафика ПКС приведено в документе RU.BATC.00178-01 34 01 «Специальное программное обеспечение подсистемы контроля сообщений автономного сегмента сети передачи данных. Руководство оператора».

А.22.3.3 В интерфейсе оператора выполнить просмотр формы ввода данных. Убедиться, что у оператора есть возможность выбора абонента путем задания совокупности коммутационно-адресных признаков, в том числе IP-адреса (10.10.10.15), IP-маски (255.255.255.0), протоколов прикладного уровня (ftp).

А.22.4 СПО ПКС считается выдержавшим испытания по п. А.22.3.1-А.22.3.3 программы и методики испытаний и выполняющим пункты 3.2.2, 3.2.2.6 ТЗ на СЧ ОКР, если оператор в интерфейсе имеет возможность выбора

абонента путем задания совокупности коммутационно-адресных признаков, в том числе IP-адреса (10.10.10.15), IP-маски (255.255.255.0), протокола (ftp).

А.23 Методика № 23

А.23.1 В данной методике проводится проверка СПО ПКС на соответствие требованиям пунктов 3.2.2, 3.2.2.7 ТЗ на СЧ ОКР «Амезит-В».

А.23.2 В соответствии с требованиями пунктов 3.2.2, 3.2.2.7 ТЗ на СЧ ОКР «Амезит-В» СПО ПКС должно обеспечивать формирование, отображение и экспорт списков абонентов-отправителей и абонентов-получателей с топологическими связями между ними.

Примечание:

1. При формировании списка должна быть предусмотрена возможность задания периода времени, за который будет производиться выбор данных для построения таблицы связей, а также возможность установки максимальной глубины рассчитываемых связей.
2. Список топологических связей между абонентами-отправителями и абонентами-получателями должен содержать информацию:

- IP-адрес абонента отправителя;
- IP-адрес абонента получателя;
- глубина связи (кол-во связующих узлов);
- состав связи (IP-адреса узлов, определяющих связь).

А.23.3 Для проведения проверки СПО ПКС на соответствие предъявляемым требованиям необходимо выполнить действия, описанные ниже.

А.23.3.1 Собрать испытательный стенд в соответствии со схемой (см. Рисунок 4).

А.23.3.2 Выполнить вход в интерфейс ПО мониторинга сетевого трафика ПКС, перейти в раздел формирования и отображения списков абонентов-отправителей и абонентов-получателей с топологическими связями между ними. Описание интерфейса ПО мониторинга сетевого трафика ПКС приведено в документе RU.ВАТС.00178-01 34 01 «Специальное программное обеспечение подсистемы контроля сообщений автономного сегмента сети передачи данных. Руководство оператора».

А.23.3.3 В интерфейсе оператора ПКС выполнить просмотр формы ввода данных. Убедиться, что оператор имеет возможность задать временной период для выбора данных, на которых следует построить таблицу топологических связей.

А.23.3.4 В интерфейсе оператора ПКС выполнить просмотр формы ввода данных. Убедиться, что оператор имеет возможность задать значение

глубины связей, которое используется для построения таблицы топологических связей.

А.23.3.5 В интерфейсе оператора ПКС выполнить команду на формирование и отображение списков абонентов-отправителей и абонентов-получателей с топологическими связями между ними. Описание команды на формирование и отображение списков абонентов-отправителей и абонентов-получателей приведено в документе RU.BATC.00178-01 92 01 «Специальное программное обеспечение подсистемы контроля сообщений автономного сегмента сети передачи данных. Руководство пользователя».

А.23.3.6 Выполнить просмотр сформированного отчета. Убедиться, что списки абонентов-отправителей и абонентов-получателей содержат информацию об IP-адресе абонента-отправителя (10.10.10.15), IP-адресе абонента-получателя (192.168.1.10), глубине связи (3), составе связи (10.10.10.144). Формирование отчета приведено в документе RU.BATC.00178-01 92 01 «Специальное программное обеспечение подсистемы контроля сообщений автономного сегмента сети передачи данных. Руководство пользователя».

А.23.4 СПО ПКС считается выдержавшим испытания по п. А.23.3.1-А.23.3.6 программы и методики испытаний и выполняющим пункты 3.2.2, 3.2.2.7 ТЗ на СЧ ОКР, если:

- в интерфейсе пользователя есть возможность задать временной период для выбора данных, на которых следует построить таблицу связей с 01.04.2018 по 01.08.2018;
- в интерфейсе пользователя есть возможность задать максимальную глубину рассчитываемых связей (3);
- в интерфейсе пользователя есть возможность выполнить формирование списков абонентов-отправителей и абонентов-получателей с топологическими связями между ними, показана связь через 10.10.10.144;
- список топологических связей между абонентами-отправителями и абонентами-получателями содержит информацию об IP-адресе абонента отправителя (10.10.10.15), IP-адресе абонента получателя (192.168.1.10).

А.24 Методика № 24

А.24.1 В данной методике проводится проверка СПО ПКС на соответствие требованиям пунктов 3.2.2, 3.2.2.8 ТЗ на СЧ ОКР «Амезит-В».

А.24.2 В соответствии с требованиями пунктов 3.2.2, 3.2.2.8 ТЗ на СЧ ОКР «Амезит-В» СПО ПКС должно обеспечивать ведение статистики сетевой активности с регистрацией сводных данных о времени контактов (с указанием

инициатора контакта), коммутационно-адресных признаках контактёров и объёмах передаваемой информации абонента, задаваемого оператором.

Примечание:

1. Статистика сетевой активности должна содержать информацию:

- дату и время начала соединения;
- дату и время завершения соединения;
- информацию о клиенте (IP, порт, доменное имя (при наличии);
- информацию о сервере (IP, порт, доменное имя (при наличии);
- код протокола в соответствии с RFC1700 либо номер порта для TCP/UDP;
- объем трафика.

2. Должна быть реализована возможность фильтрации, сортировки и экспорта сетевой статистики.

А.24.3 Для проведения проверки СПО ПКС на соответствие предъявляемым требованиям необходимо выполнить действия, описанные ниже.

А.24.3.1 Собрать испытательный стенд в соответствии со схемой (см. рисунок Рисунок 4).

А.24.3.2 Выполнить вход в интерфейс ПО мониторинга сетевого трафика ПКС, перейти в раздел отображения сетевой активности. Описание интерфейса ПО мониторинга сетевого трафика ПКС приведено в документе RU.BATC.00178-01 34 01 «Специальное программное обеспечение подсистемы контроля сообщений автономного сегмента сети передачи данных. Руководство оператора».

А.24.3.3 Выполнить команду на формирование отчета по сетевой статистике и путем просмотра отчета убедиться, что выполняется регистрация сводных данных о времени контактов (с указанием инициатора контакта), коммутационно-адресных признаках контактеров и объемах передаваемой информации абонента. Описание команды на формирование отчета по сетевой статистики приведено в документе RU.BATC.00178-01 92 01 «Специальное программное обеспечение подсистемы контроля сообщений автономного сегмента сети передачи данных. Руководство пользователя».

А.24.3.4 Выполнить просмотр сформированного отчета. Убедиться, что статистика о сетевой активности содержит информацию о дате и времени начала соединения, дате и времени завершения соединения, информацию о клиенте (IP, порт), информацию о сервере (IP, порт), код протокола в соответствии с RFC1700 либо номер порта для TCP/UDP, объем трафика. Описание формирования отчета приведено в документе RU.BATC.00178-01 92

01 «Специальное программное обеспечение подсистемы контроля сообщений автономного сегмента сети передачи данных. Руководство пользователя».

А.24.3.5 Выполнить фильтрацию, сортировку и экспорт сформированного отчета. Описание выполнения фильтрации, сортировки и экспорта сформированного отчета приведено в документе RU.BATC.00178-01 92 01 «Специальное программное обеспечение подсистемы контроля сообщений автономного сегмента сети передачи данных. Руководство пользователя».

А.24.3.6 Выполнить просмотр сформированного отчета. Убедиться, что в соответствии с командами выполняется фильтрация, сортировка отчета и экспорт отчета в файл. Описание формирования отчета приведено в документе RU.BATC.00178-01 92 01 «Специальное программное обеспечение подсистемы контроля сообщений автономного сегмента сети передачи данных. Руководство пользователя».

А.24.4 СПО ПКС считается выдержавшим испытания по п. А.24.3.1-А.24.3.6 программы и методики испытаний и выполняющим пункты 3.2.2, 3.2.2.8 ТЗ на СЧ ОКР, если:

- в интерфейсе пользователя выполняется регистрация времени контакта (14:56:10), коммутационно-адресных признаках контактеров (10.10.10.15 и 192.168.1.10) и объемах передаваемой информации абонента (105300 байт);
- в интерфейсе пользователя есть возможность фильтрации, сортировки и экспорта сформированного отчета;
- в интерфейсе пользователя есть возможность просмотра статистики сетевых соединений, которая содержит информацию о времени начала соединения (14:56:10), о времени окончания соединения (15:06:02), о клиенте (10.10.10.15 : 21), информацию о сервере (192.168.1.10), код протокола (ftp) объем трафика (105300 байт).

А.25 Методика № 25

А.25.1 В данной методике проводится проверка СПО ПКС на соответствие требованиям пунктов 3.2.2, 3.2.2.9 ТЗ на СЧ ОКР «Амезит-В».

А.25.2 В соответствии с требованиями пунктов 3.2.2, 3.2.2.9 ТЗ на СЧ ОКР «Амезит-В» СПО ПКС должно обеспечивать регистрацию в накопитель информационного обмена (в полном объеме) для абонента, задаваемого оператором.

А.25.3 Для проведения проверки СПО ПКС на соответствие предъявляемым требованиям необходимо выполнить действия, описанные ниже.

А.25.3.1 Собрать испытательный стенд в соответствии со схемой (см. рисунок Рисунок 4).

А.25.3.2 Выполнить подключение генератора трафика (АПК СКАТ) к испытательному стенду. Порядок подключения генератора трафика (АПК СКАТ) и настройки испытательного стенда приведен в документе RU.BATC.00178-01 32 01 «Специальное программное обеспечение подсистемы контроля сообщений автономного сегмента сети передачи данных. Руководство системного программиста».

А.25.3.3 Выполнить запуск генератора трафика, который обеспечивает устойчивый информационный обмен от имени выбранного абонента, проходящий через ПО мониторинга сетевого трафика ПКС. Инструкции по работе с генератором трафика приведены в документе RU.BATC.00178-01 32 01 «Специальное программное обеспечение подсистемы контроля сообщений автономного сегмента сети передачи данных. Руководство системного программиста».

А.25.3.4 Выполнить вход в интерфейс оператора ПО мониторинга сетевого трафика ПКС, перейти в раздел настройки правил отбора материалов информационного обмена. Описание интерфейса ПО мониторинга сетевого трафика ПКС приведено в документе RU.BATC.00178-01 34 01 «Специальное программное обеспечение подсистемы контроля сообщений автономного сегмента сети передачи данных. Руководство оператора».

А.25.3.5 В интерфейсе оператора выполнить ввод правил отбора материалов информационного обмена для выбранного абонента. Указать IP адрес 10.10.10.15 и протокол ftp.

А.25.3.6 В интерфейсе оператора перейти в раздел просмотра сохраненного трафика.

А.25.3.7 Выполнить просмотр файлов, содержащих сохраненный трафик. Убедиться, что материалы информационного обмена абонента, заданного оператором, сохранены в виде отдельных файлов (file2036).

А.25.3.8 В интерфейсе оператора перейти в раздел просмотра статистики соединений.

А.25.3.9 Выполнить просмотр статистики соединений абонента, выбранного оператором, и сравнение размеров файлов, содержащих сохраненный трафик, с объемом переданного трафика из статистики соединений. Убедиться, что информационный обмен абонента, заданного оператором, зарегистрирован в накопитель информационного обмена в полном объеме. Просмотр статистики соединений абонента приведен в документе RU.BATC.00178-01 92 01 «Специальное программное обеспечение подсистемы

контроля сообщений автономного сегмента сети передачи данных. Руководство пользователя».

А.25.4 СПО ПКС считается выдержавшим испытания по п. А.25.3.1-А.25.3.9 программы и методики испытаний и выполняющим пункты 3.2.2, 3.2.2.9 ТЗ на СЧ ОКР, если:

- в интерфейсе пользователя выполняется настройка правил съема трафика на указанного абонента (IP адрес 10.10.10.15 и протокол FTP);

- в течение сеанса работы абонента выполнялся съем и сохранение информационного обмена абонента (появился файл с сохраненным трафиком file2036_pcap).

А.26 Методика № 26

А.26.1 В данной методике проводится проверка СПО ПКС на соответствие требованиям пунктов 3.2.2, 3.2.2.10 ТЗ на СЧ ОКР «Амезит-В».

А.26.2 В соответствии с требованиями пунктов 3.2.2, 3.2.2.10 ТЗ на СЧ ОКР «Амезит-В» СПО ПКС должно обеспечивать визуализацию трафика и анализ связей участников соединений до требуемого уровня (построение графов связи по МАС-адресам, IP-адресам, адресам электронной почты (при наличии статистики почтовых соединений)).

Примечания:

1. При построении графов для визуализации трафика должна быть возможность задать временной период для выбора данных, на которых следует строить граф.

2. Изображение графа связей абонентов по МАС-адресам должно содержать:

- узлы, показанные в виде МАС-адресов;
- связи, построенные на основании статистики соединений.

3. Изображение графа связей абонентов по IP-адресам должно содержать:

- узлы, показанные в виде IP-адресов;
- связи, построенные на основании статистики соединений.

4. Граф соединений по e-mail должен строиться на основании статистики почтовых сообщений, которая формируется из перехваченного почтового трафика из полей: отправитель почтового сообщения, список получателей почтового сообщения, список получателей копии почтового сообщения.

5. Изображение графа связей абонентов по e-mail должно содержать:

- узлы, показанные в виде email адресов;
- связи, построенные на основании статистики почтовых сообщений.

6. Должна быть предусмотрена возможность экспорта полученных изображений графов.

7. При построении графа связей абонентов должна быть предусмотрена возможность асинхронного получения доменного имени по IP-адресу (при его наличии).

А.26.3 Для проведения проверки СПО ПКС на соответствие предъявляемым требованиям необходимо выполнить действия, описанные ниже.

А.26.3.1 Собрать испытательный стенд в соответствии со схемой (см. рисунок Рисунок 4).

А.26.3.2 Выполнить вход в интерфейс ПО мониторинга сетевого трафика ПКС, перейти в раздел построения графа связи по MAC-адресам. Описание интерфейса раздела приведено в документе RU.BATC.00178-01 34 01 «Специальное программное обеспечение подсистемы контроля сообщений автономного сегмента сети передачи данных. Руководство оператора».

А.26.3.3 Задать временной период для выбора данных, для которых следует построить граф в интерфейсе раздела построения графа связи по MAC-адресам.

А.26.3.4 Выполнить команду на построение графа связи по MAC-адресам. Выполнить просмотр сформированного отчета. Убедиться, что выполняется визуализация связей по MAC-адресам в виде графа, в котором узлы показаны в виде MAC-адресов (адрес в виде e0:db:55:d5:a9:0c), а связи построены на основании статистики соединений.

А.26.3.5 В интерфейсе оператора перейти в раздел построения графа связи по MAC-адресам.

А.26.3.6 Выполнить команду на построение графа связей абонентов по IP-адресам (1.100.158.180). Выполнить просмотр сформированного отчета. Убедиться, что выполняется визуализация связей по IP-адресам в виде графа, в котором узлы показаны в виде IP-адресов (1.100.158.180 и 1.10.30.90), а связи построены на основании статистики соединений. Проверить, что при выборе IP-адреса 1.100.158.180 показывается доменное имя: uhtainkebbv.com.

А.26.3.7 В интерфейсе оператора перейти в раздел построения графа соединений по e-mail-адресам.

А.26.3.8 Выполнить команду на построение графа соединений по e-mail-адресам. Выполнить просмотр сформированного отчета. Убедиться, что выполняется визуализация связей по e-mail-адресам в виде графа, в котором узлы показаны в виде e-mail-адресов, а связи построены на основании статистики почтовых соединений из полей: отправитель почтового сообщения,

список получателей почтового сообщения, список получателей копии почтового сообщения (btvjtqnb.edu и uhtainkebbv.com).

A.26.4 СПО ПКС считается выдержавшим испытания по п. А.26.3.1-А.26.3.8 программы и методики испытаний и выполняющим пункты 3.2.2, 3.2.2.10 ТЗ на СЧ ОКР, если в интерфейсе пользователя есть возможность:

- задать временной период для выбора данных, на которых следует строить граф;
- выполнить визуализацию связей по MAC-адресам (адрес в виде e0:db:55:d5:a9:0c) в виде графа, в котором узлы показаны в виде MAC-адресов;
- выполнить визуализацию связей по IP-адресам в виде графа, в котором узлы показаны в виде IP-адресов (1.100.158.180 и 1.10.30.90);
- выполнить визуализацию связей по e-mail-адресам в виде графа, в котором узлы показаны в виде e-mail-адресов (btvjtqnb.edu и uhtainkebbv.com);
- экспорта изображений графов в файлы png;
- получения доменного имени по IP-адресу (при его наличии) (1.100.158.180 - uhtainkebbv.com).

A.27 Методика № 27

A.27.1 В данной методике проводится проверка СПО ПКС на соответствие требованиям пунктов 3.2.2, 3.2.2.11 ТЗ на СЧ ОКР «Амезит-В».

A.27.2 В соответствии с требованиями пунктов 3.2.2, 3.2.2.11 ТЗ на СЧ ОКР «Амезит-В» СПО ПКС должно обеспечивать осуществление распределенных вычислений в целях поиска ключевой информации к следующим типам файлов:

- к технически закрытым файлам: форматов DOC, DOCX, XLS, XLSX, PPT, PPTX, PDF, ZIP, RAR;
- технически закрытым файлам, закрытым с помощью алгоритмов DES, TripleDES, AES 128, AES256; к хеш-функциям md5 и sha-1.

Примечание:

1. В качестве технологии построения узла обработки № 1 должна использоваться FPGA (с возможностью дополнения технологией GPU).
2. В качестве технологии построения узла обработки № 2 должен использоваться GPU.
3. Должна быть реализована возможность осуществления распределенных вычислений на базе технических средств, входящих в состав комплекса (в том числе, территориально удаленных друг от друга с использованием подсистемы ППД), с использованием ПО типа Elcomsoft Password Recovery Bundle.
4. Должна быть предусмотрена возможность масштабирования узлов обработки путем наращивания технических средств.

А.27.3 Для проведения проверки СПО ПКС на соответствие предъявляемым требованиям необходимо выполнить действия, описанные ниже.

А.27.3.1 Собрать испытательный стенд в соответствии со схемой (см. рисунок Рисунок 4).

А.27.3.2 Выполнить вход в интерфейс оператора ПО поиска ключевой информации ПКС узла обработки № 1. Задать исходную директорию, место сохранения результатов обработки и параметры задания на обработку. Описание интерфейса ПО поиска ключевой информации ПКС приведено в документе RU.ВАТС.00178-01 34 01 «Специальное программное обеспечение подсистемы контроля сообщений автономного сегмента сети передачи данных. Руководство оператора».

А.27.3.3 Разместить в исходной директории ПО поиска ключевой информации ПКС узла обработки № 1 (построенного на базе FPGA) набор тестовых данных (testdatafpga), представляющих множество файлов (форматов DOC, DOCX, XLS, XLSX, PPT, PPTX, PDF, ZIP, RAR), каждый из которых закрыт с помощью алгоритмов DES, TripleDES, AES 128, AES 256, хеш-функций md5, sha-1. Дождаться окончания процедуры поиска ключевой информации. Инструкции по настройке исходных директорий и параметров работы СПО поиска ключевой информации приведены в документе RU.ВАТС.00178-01 32 01 «Специальное программное обеспечение подсистемы контроля сообщений автономного сегмента сети передачи данных. Руководство системного программиста».

А.27.3.4 Выполнить просмотр записей журналов обработки ПО поиска ключевой информации ПКС узла обработки № 1. Убедиться, что для файлов, входящих в тестовый массив данных testdatafpga, найдена ключевая информация (файл fpga001 (форматов DOC, DOCX, XLS, XLSX, PPT, PPTX, PDF, ZIP, RAR)). Поиск ключевой информации описан в документе RU.ВАТС.00178-01 92 01 «Специальное программное обеспечение подсистемы контроля сообщений автономного сегмента сети передачи данных. Руководство пользователя».

А.27.3.5 Выполнить вход в интерфейс оператора ПО поиска ключевой информации ПКС узла обработки № 2, задать исходную директорию, место сохранения результатов обработки и параметры задания на обработку.

А.27.3.6 Разместить в исходной директории ПО поиска ключевой информации ПКС узла обработки № 2 (построенного на базе GPU) набор тестовых данных (testdatagpu), представляющих множество файлов (форматов DOC, DOCX, XLS, XLSX, PPT, PPTX, PDF, ZIP, RAR), каждый из которых

закрыт с помощью алгоритмов DES, TripleDES, AES 128, AES 256, хеш-функций md5, sha-1. Дождаться окончания процедуры поиска ключевой информации. Поиск ключевой информации описан в документе RU.ВАТС.00178-01 92 01 «Специальное программное обеспечение подсистемы контроля сообщений автономного сегмента сети передачи данных. Руководство пользователя».

А.27.3.7 Выполнить просмотр записей журналов обработки СПО поиска ключевой информации ПКС узла обработки № 2; убедиться, что для файлов, входящих в тестовый массив данных testdatagpu, найдена ключевая информация (файл gpu001 (форматов DOC, DOCX, XLS, XLSX, PPT, PPTX, PDF, ZIP, RAR)). Просмотр записей журналов обработки СПО поиска ключевой информации ПКС описан в документе RU.ВАТС.00178-01 92 01 «Специальное программное обеспечение подсистемы контроля сообщений автономного сегмента сети передачи данных. Руководство пользователя».

А.27.4 СПО ПКС считается выдержавшим испытания по п. А.27.3.1-А.27.3.7 программы и методики испытаний и выполняющим пункты 3.2.2, 3.2.2.11 ТЗ на СЧ ОКР, если:

- обеспечивается осуществление распределенных вычислений;
- пользователь при помощи СПО поиска ключевой информации ПКС узла обработки № 1 (построенного на базе FPGA) и СПО поиска ключевой информации ПКС узла обработки № 2 (построенного на базе GPU) может выполнить поиск ключевой информации в защифрованных тестовых наборах testdatafpga и testdatagpu и получить файлы fpga001 (форматов DOC, DOCX, XLS, XLSX, PPT, PPTX, PDF, ZIP, RAR) и gpu001 (форматов DOC, DOCX, XLS, XLSX, PPT, PPTX, PDF, ZIP, RAR).

А.28 Методика № 28

А.28.1 В данной методике проводится проверка СПО ПМС на соответствие требованиям пунктов 3.2.3, 3.2.3.1 ТЗ на СЧ ОКР «Амезит-В».

А.28.2 В соответствии с требованиями пунктов 3.2.3, 3.2.3.1 ТЗ на СЧ ОКР «Амезит-В» СПО ПМС должно обеспечивать сбор информации из следующих социальных сетей, блогов, микроблогов, форумов, а также новостных информационных порталов в заданном географическом регионе:

- Вконтакте;
- Facebook;
- Мой мир@mail.ru;
- Одноклассники;
- LiveJournal;

- Twitter;
- Google+;
- Youtube;
- Diary.ru;
- Liveinternet.ru;
- BlogSpot;
- Tumblr;
- Renren Network;
- Веб-страницы сети Интернет и СМИ.

А.28.2.1 Сбор информации из социальной сети ВКонтакте должен включать следующие данные:

- заголовки постов;
- тексты постов;
- URL-постов;
- имена авторов постов;
- URL профиля авторов постов;
- географическое расположение (при наличии технической возможности) авторов постов;
- тексты репостов (при наличии технической возможности) постов;
- URL репостов постов;
- количество репостов;
- тексты комментариев (при наличии технической возможности) постов;
- количество комментариев;
- дата публикации постов;
- медиа (фото, видео, аудио, прикрепленных к посту, при наличии технической возможности).

А.28.2.2 Сбор информации из социальной сети Facebook должен включать следующие данные:

- заголовки постов;
- тексты постов;
- URL-постов;
- имена авторов постов;
- URL профиля авторов постов;
- географическое расположение (при наличии технической возможности) авторов постов;
- тексты репостов (при наличии технической возможности) постов;
- URL репостов постов;
- количество репостов;

- тексты комментариев (при наличии технической возможности) постов;
- количество комментариев;
- дата публикации постов;
- медиа (фото, видео, аудио, прикрепленных к посту, при наличии технической возможности).

А.28.2.3 Сбор информации из социальной сети Мой Мир@mail.ru должен включать следующие данные:

- заголовки постов;
- тексты постов;
- URL-постов;
- имена авторов постов;
- URL профиля авторов постов;
- географическое расположение (при наличии технической возможности) авторов постов;
- тексты репостов (при наличии технической возможности) постов;
- URL репостов постов;
- количество репостов;
- тексты комментариев (при наличии технической возможности) постов;
- количество комментариев;
- дата публикации постов;
- медиа (фото, видео, аудио, прикрепленных к посту, при наличии технической возможности).

А.28.2.4 Сбор информации из социальной сети Одноклассники должен включать следующие данные:

- заголовки постов;
- тексты постов;
- URL-постов;
- имена авторов постов;
- URL профиля авторов постов;
- географическое расположение (при наличии технической возможности) авторов постов;
- тексты репостов (при наличии технической возможности) постов;
- URL репостов постов;
- количество репостов;
- тексты комментариев (при наличии технической возможности) постов;
- количество комментариев;
- дата публикации постов;

- медиа (фото, видео, аудио, прикрепленных к посту, при наличии технической возможности).

А.28.2.5 Сбор информации из социальной сети LiveJournal должен включать следующие данные:

- заголовки постов;
- тексты постов;
- URL-постов;
- имена авторов постов;
- URL профиля авторов постов;
- географическое расположение (при наличии технической возможности) авторов постов;
- тексты репостов (при наличии технической возможности) постов;
- URL репостов постов;
- количество репостов;
- тексты комментариев (при наличии технической возможности) постов;
- количество комментариев;
- дата публикации постов;
- медиа (фото, видео, аудио, прикрепленных к посту, при наличии технической возможности).

А.28.2.6 Сбор информации из социальной сети Twitter должен включать следующие данные:

- заголовки постов;
- тексты постов;
- URL-постов;
- имена авторов постов;
- URL профиля авторов постов;
- географическое расположение (при наличии технической возможности) авторов постов;
- тексты репостов (при наличии технической возможности) постов;
- URL репостов постов;
- количество репостов;
- тексты комментариев (при наличии технической возможности) постов;
- количество комментариев;
- дата публикации постов;
- хэштэги поста – краткое название, идентифицирующее тематику поста;
- медиа (фото, видео, аудио, прикрепленных к посту, при наличии технической возможности).

Сбор информации из социальной сети Google+ должен включать следующие данные:

- заголовки постов;
- тексты постов;
- URL-постов;
- имена авторов постов;
- URL профиля авторов постов;
- географическое расположение (при наличии технической возможности) авторов постов;
- тексты репостов (при наличии технической возможности) постов;
- URL репостов постов;
- количество репостов;
- тексты комментариев (при наличии технической возможности) постов;
- количество комментариев;
- дата публикации постов;
- медиа (фото, видео, аудио, прикрепленных к посту, при наличии технической возможности).

А.28.2.7 Сбор информации из социальной сети Youtube должен включать следующие данные:

- видео;
- название видео;
- URL видео;
- имена авторов видео;
- URL профиля авторов видео;
- географическое расположение (при наличии технической возможности) авторов постов;
- тексты комментариев (при наличии технической возможности) к видео;
- количество комментариев.

А.28.2.8 Сбор информации из социальной сети Diary.ru должен включать следующие данные:

- заголовки постов;
- тексты постов;
- URL-постов;
- имена авторов постов;
- URL профиля авторов постов;
- географическое расположение (при наличии технической возможности) авторов постов;

- тексты репостов (при наличии технической возможности) постов;
- URL репостов постов;
- количество репостов;
- тексты комментариев (при наличии технической возможности) постов;
- количество комментариев;
- дата публикации постов;
- медиа (фото, видео, аудио, прикрепленных к посту, при наличии технической возможности).

А.28.2.9 Сбор информации из социальной сети Liveinternet.ru должен включать следующие данные:

- заголовки постов;
- тексты постов;
- URL-постов;
- имена авторов постов;
- URL профиля авторов постов;
- географическое расположение (при наличии технической возможности) авторов постов;
- тексты репостов (при наличии технической возможности) постов;
- URL репостов постов;
- количество репостов;
- тексты комментариев (при наличии технической возможности) постов;
- количество комментариев;
- дата публикации постов;
- медиа (фото, видео, аудио, прикрепленных к посту, при наличии технической возможности).

А.28.2.10 Сбор информации из социальной сети BlogSpot должен включать следующие данные:

- заголовки постов;
- тексты постов;
- URL-постов;
- имена авторов постов;
- URL профиля авторов постов;
- географическое расположение (при наличии технической возможности) авторов постов;
- тексты репостов (при наличии технической возможности) постов;
- URL репостов постов;
- количество репостов;
- тексты комментариев (при наличии технической возможности) постов;

- количество комментариев;
- дата публикации постов;
- медиа (фото, видео, аудио, прикрепленных к посту, при наличии технической возможности).

А.28.2.11 Сбор информации из социальной сети Tumblr должен включать следующие данные:

- заголовки постов;
- тексты постов;
- URL-постов;
- имена авторов постов;
- URL профиля авторов постов;
- географическое расположение (при наличии технической возможности) авторов постов;
- тексты репостов (при наличии технической возможности) постов;
- URL репостов постов;
- количество репостов;
- тексты комментариев (при наличии технической возможности) постов;
- количество комментариев;
- дата публикации постов;
- медиа (фото, видео, аудио, прикрепленных к посту, при наличии технической возможности).

А.28.2.12 Сбор информации из социальной сети Renren Network должен включать следующие данные:

- заголовки постов;
- тексты постов;
- URL-постов;
- имена авторов постов;
- URL профиля авторов постов;
- географическое расположение (при наличии технической возможности) авторов постов;
- тексты репостов (при наличии технической возможности) постов;
- URL репостов постов;
- количество репостов;
- тексты комментариев (при наличии технической возможности) постов;
- количество комментариев;
- дата публикации постов;
- медиа (фото, видео, аудио, прикрепленных к посту, при наличии технической возможности).

А.28.2.13 Сбор информации из сети Интернет и СМИ должен включать следующие данные:

- заголовки статей;
- тексты статей;
- URL статей;
- географические данные (при наличии технической возможности) статей;
- IP-адрес (при наличии технической возможности) статей;
- имя авторов (при наличии технической возможности) статей;
- URL профиля авторов статей;
- географическое расположение (при наличии технической возможности) авторов постов;
- тексты репостов (при наличии технической возможности) постов;
- URL репостов статей;
- количество репостов статей;
- тексты комментариев (при наличии технической возможности) статей;
- количество комментариев статей;
- хэштеги статей – краткое название, идентифицирующее тематику статей;
- дата публикации статей;
- медиа (фото, видео, аудио, прикрепленных к посту, при наличии технической возможности).

А.28.3 Для проведения проверки СПО ПМС на соответствие предъявляемым требованиям необходимо выполнить действия, описанные ниже.

А.28.3.1 На рабочем столе АРМ оператора запустить обозреватель.

А.28.3.2 В адресной строке ввести адрес сервера приложений и нажать на клавишу «Enter». Адрес сервера приложений уточняется после установки и настройки СПО ПМС согласно документу RU.BATC.00179-01 32 01 «Специальное программное обеспечение подсистемы мониторинга сети Интернет и СМИ. Руководство системного программиста». Откроется страница авторизации.

А.28.3.3 На странице авторизации ввести аутентификационные данные (логин: admin, пароль: password) и нажать на кнопку «Войти». Откроется стартовая страница с отслеживаемыми тематиками. Описание интерфейса СПО ПМС приведено в документе RU.BATC.00179-01 92 01 «Специальное программное обеспечение подсистемы мониторинга сети Интернет и СМИ. Руководство пользователя».

А.28.3.4 В верхней части страницы нажать на строку поиска. Откроется панель фильтров.

А.28.3.5 На панели фильтров в поле «Источник» выбрать источник публикации «vk.com».

А.28.3.6 На панели фильтров в поле «Страна» выбрать страну публикаций «Россия» в качестве региона публикации.

А.28.3.7 Закрыть панель фильтров, нажав на кнопку «Закрыть». Отображаются публикации из социальной сети ВКонтакте в России.

А.28.4 СПО ПМС считается выдержавшим испытания по п. А.28.3.1-А.28.3.7 программы и методики испытаний и выполняющим пункты 3.2.3, 3.2.3.1 ТЗ на СЧ ОКР «Амезит-В», если:

- в списке публикаций отобразились публикации;
- возле каждой публикации в поле «Локации» отобразился только выбранный регион «Россия»;
- возле каждой публикации в поле «Источник» отобразился только выбранный источник «vk.com» (ВКонтакте);
- информация о каждой публикации содержит данные, указанные в пункте 3.2.3.1 ТЗ на СЧ ОКР «Амезит-В» для выбранного источника публикаций.

А.29 Методика № 29

А.29.1 В данной методике проводится проверка СПО ПМС на соответствие требованиям пунктов 3.2.3, 3.2.3.2 ТЗ на СЧ ОКР «Амезит-В».

А.29.2 В соответствии с требованиями пунктов 3.2.3, 3.2.3.2 ТЗ на СЧ ОКР «Амезит-В» СПО ПМС должно обеспечивать выявление источника появления информации.

А.29.3 Для проведения проверки СПО ПМС на соответствие предъявляемым требованиям необходимо выполнить действия, описанные ниже.

А.29.3.1 Повторить пункты с А.28.3.1 по А.28.3.7 (Методика № 28).

А.29.3.2 В списке публикаций нажать на значок «Граф распространения публикаций». Откроется страница, на которой изображен граф распространения публикаций.

А.29.3.3 На графе распространения публикаций нажать на крайнюю левую вершину графа. Откроется страница с графом и данными публикации, которая является первоисточником.

А.29.4 СПО ПМС считается выдержавшим испытания по п. А.29.3.1-А.29.3.3 программы и методики испытаний и выполняющим пункты 3.2.3, 3.2.3.2 ТЗ на СЧ ОКР, если:

- отобразился граф распространения публикаций со шкалой времени и крайней левой вершиной – первоисточником публикаций;
- при нажатии на крйнюю левую вершину графа, являющуюся первоисточником, открылась страница, содержащая следующую информацию о публикации: автор, текст, дата публикации, ссылка на источник в сети Интернет.

А.30 Методика № 30

А.30.1 В данной методике проводится проверка СПО ПМС на соответствие требованиям пунктов 3.2.3, 3.2.3.3 ТЗ на СЧ ОКР «Амезит-В».

А.30.2 В соответствии с требованиями пунктов 3.2.3, 3.2.3.3 ТЗ на СЧ ОКР «Амезит-В» СПО ПМС должно обеспечивать анализ распространения информации с представлением результатов в графическом виде (в виде графа распространения).

А.30.3 Для проведения проверки СПО ПМС на соответствие предъявляемым требованиям необходимо выполнить действия, описанные ниже.

А.30.3.1 Повторить пункты с А.28.3.1 по А.28.3.7 (Методика № 28).

А.30.3.2 В списке публикаций нажать на значок «Граф распространения публикаций». Откроется окно, в котором изображен граф распространения публикаций. Описание интерфейса СПО ПМС приведено в документе RU.BATC.00179-01 92 01 «Специальное программное обеспечение подсистемы мониторинга сети Интернет и СМИ. Руководство пользователя».

А.30.4 СПО ПМС считается выдержавшим испытания по п. А.30.3.1-А.30.3.2 программы и методики испытаний и выполняющим пункты 3.2.3, 3.2.3.3 ТЗ на СЧ ОКР, если:

- отобразился граф распространения публикаций;
- вершины графа расположены в хронологическом порядке в соответствии со шкалой времени, начиная с крайней левой вершины вершины – первоисточника информации.

А.31 Методика № 31

А.31.1 В данной методике проводится проверка СПО ПМС на соответствие требованиям пунктов 3.2.3, 3.2.3.4 ТЗ на СЧ ОКР «Амезит-В».

А.31.2 В соответствии с требованиями пунктов 3.2.3, 3.2.3.4 ТЗ на СЧ ОКР «Амезит-В» СПО ПМС должно обеспечивать анализ эмоциональной окраски информационных материалов.

А.31.3 Для проведения проверки СПО ПМС на соответствие предъявляемым требованиям необходимо выполнить действия, описанные ниже.

А.31.3.1 Повторить пункты с А.28.3.1 по А.28.3.7 (Методика № 28).

А.31.4 СПО ПМС считается выдержавшим испытания по п. А.31.3.1 программы и методики испытаний и выполняющим пункты 3.2.3, 3.2.3.4 ТЗ на СЧ ОКР, если:

- отобразился значок эмоциональной окраски возле каждой публикации, для которой произведена оценка тональности текста;

- при наведении указателя мыши на значок эмоциональной окраски отобразилось число, обозначающее тональность публикации в диапазоне от -1 до 1;

- значок эмоциональной окраски имеет цветовую маркировку в зависимости от значения тональности – от красного (-1) до зеленого (1). Нейтральная окраска (0) обозначена черным цветом.

А.32 Методика № 32

А.32.1 В данной методике проводится проверка СПО ПМС на соответствие требованиям пунктов 3.2.3, 3.2.3.5 ТЗ на СЧ ОКР «Амезит-В».

А.32.2 В соответствии с требованиями пунктов 3.2.3, 3.2.3.5 ТЗ на СЧ ОКР «Амезит-В» СПО ПМС должно обеспечивать непрерывный целевой поиск и отбор разнородной информации в цифровых источниках открытого доступа по заданной тематической направленности с осуществлением географической идентификации, ее совместный комплексный анализ на геопространственной основе.

А.32.3 Для проведения проверки СПО ПМС на соответствие предъявляемым требованиям необходимо выполнить действия, описанные ниже.

А.32.3.1 Повторить пункты с А.28.3.1 по А.28.3.7 (Методика № 28).

А.32.3.2 В правой верхней части страницы нажать на значок меню.

А.32.3.3 В выпадающем меню выбрать пункт «Тематики». Откроется страница со списком тематик, по которым происходит сбор информации.

А.32.3.4 Нажать на кнопку «Добавить» для создания новой тематики. Откроется окно создания тематики.

А.32.3.5 В открывшемся окне ввести:

- в поле «Название» – название тематики;

- в поле «Ключевые слова» – список слов или словосочетаний, по которым осуществляется поиск публикаций;

- в поле «Исключаемые слова» – список слов или словосочетаний, по которым публикации исключаются из сбора.

А.32.3.6 Нажать на кнопку «Сохранить».

А.32.3.7 В левой верхней части страницы нажать на значок для перехода на стартовую страницу. Откроется стартовая страница, содержащая список отслеживаемых тематик.

А.32.3.8 В списке отслеживаемых тематик нажать на созданную тематику публикаций. Откроется список всех собранных публикаций по данной тематике.

А.32.3.9 Подождать, пока не придет уведомление о новых собранных публикациях (от 5 до 30 минут).

А.32.3.10 В верхней части страницы нажать на значок уведомлений для раскрытия списка доступных уведомлений.

А.32.3.11 В списке уведомлений нажать на уведомление с текстом «Найдено X новых публикаций по тематике Y», где X – количество новых публикаций, Y – название тематики.

А.32.3.12 Перезагрузить страницу, нажав на клавишу F5 на клавиатуре. В списке публикаций отобразятся новые публикации.

А.32.3.13 На странице со списком публикаций нажать на значок карты. Откроется карта мира, где маркерами отмечены публикации по данной тематике.

А.32.4 СПО ПМС считается выдержавшим испытания по п. А.32.3.1-А.32.3.13 программы и методики испытаний и выполняющим пункты 3.2.3, 3.2.3.5 ТЗ на СЧ ОКР, если:

- на стартовой странице отобразилась новая созданная тематика;
- пришло уведомление о появлении новых публикаций по созданной тематике;
- в начале списка публикаций отобразились новые публикации по выбранной тематике;
- публикации содержат данные о регионе публикации, если была возможность выделить его в процессе сбора или при анализе текста;
- публикации, у которых определен регион публикации, отобразились на карте публикаций.

А.33 Методика № 33

А.33.1 В данной методике проводится проверка СПО ПМС на соответствие требованиям пунктов 3.2.3, 3.2.3.6 ТЗ на СЧ ОКР «Амезит-В».

А.33.2 В соответствии с требованиями пунктов 3.2.3, 3.2.3.6 ТЗ на СЧ ОКР «Амезит-В» СПО ПМС должно обеспечивать визуализацию обобщенных результатов тематического отбора информации из открытых цифровых источников на цифровой интерактивной модели земного шара (ГИС) с возможностью детализации интересующих материалов и их отбора.

А.33.3 Для проведения проверки СПО ПМС на соответствие предъявляемым требованиям необходимо выполнить действия, описанные ниже.

А.33.3.1 Повторить пункты с А.32.3.1 по А.32.3.8 (Методика № 32).

А.33.3.2 На странице со списком публикаций нажать на значок карты. Откроется карта мира, где маркерами отмечены публикации по данной тематике.

А.33.3.3 В верхней части страницы нажать на строку поиска. Откроется панель фильтров.

А.33.3.4 На панели фильтров в поле «Страна» выбрать страну публикаций «Россия» в качестве региона публикации.

А.33.3.5 Закрыть панель фильтров, нажав на кнопку «Закрыть». На карте отобразятся публикации из России.

А.33.3.6 Нажать на маркер публикации. Отобразятся атрибуты публикации: автор, текст, дата публикации, ссылка на источник в сети Интернет.

А.33.4 СПО ПМС считается выдержавшим испытания по п. А.33.3.1-А.33.3.6 программы и методики испытаний и выполняющим пункты 3.2.3, 3.2.3.6 ТЗ на СЧ ОКР, если:

- на карте публикаций отобразились публикации по выбранной тематике и по выбранному фильтру;
- после нажатия на метку публикации на карте отобразились атрибуты публикации: автор, текст, дата публикации, ссылка на источник в сети Интернет.

А.34 Методика № 34

А.34.1 В данной методике проводится проверка СПО ПМС на соответствие требованиям пунктов 3.2.3, 3.2.3.7 ТЗ на СЧ ОКР «Амезит-В».

А.34.2 В соответствии с требованиями пунктов 3.2.3, 3.2.3.7 ТЗ на СЧ ОКР «Амезит-В» СПО ПМС должно обеспечивать формирование шаблонов обработки цифровых источников открытого доступа с указанием регионов, информацию в которых необходимо собирать.

Примечание. Шаблоны цифровых источников открытого доступа должны состоять из следующих регионов:

- заголовок статьи;
- автор статьи;
- текст статьи;
- ссылка на источник материала;
- дата публикации статьи;
- геоданные по статье;
- хештэги статьи – краткое название, идентифицирующее тематику статьи);
- медиа (фото, видео, аудио, прикрепленных к статье);
- комментарии статьи.

А.34.3 Для проведения проверки СПО ПМС на соответствие предъявляемым требованиям необходимо выполнить действия, описанные ниже.

А.34.3.1 На рабочем столе АРМ оператора запустить обозреватель.

А.34.3.2 В адресной строке ввести адрес новостного сайта «Lenta.Ru»: www.lenta.ru. Откроется домашняя страница данного сайта.

А.34.3.3 На домашней странице новостного сайта «Lenta.Ru» перейти на одну из новостных статей. Откроется страница с выбранной статьей.

А.34.3.4 В верхней части обозревателя нажать на значок расширения «Шаблонизатор». Откроется окно расширения «Шаблонизатор» по формированию или редактированию шаблона обработки ресурса.

А.34.3.5 Выполнить действия по редактированию шаблона обработки информации согласно документу RU.ВАТС.00179-01 92 01 «Специальное программное обеспечение подсистемы мониторинга сети Интернет и СМИ. Руководство пользователя».

А.34.4 СПО ПМС считается выдержавшим испытания по п. А.34.3.1-А.34.3.5 программы и методики испытаний и выполняющим пункты 3.2.3, 3.2.3.7 ТЗ на СЧ ОКР, если в процессе редактирования шаблона не возникло ошибок.

А.35 Методика № 35

А.35.1 В данной методике проводится проверка СПО ПМС на соответствие требованиям пунктов 3.2.3, 3.2.3.8 ТЗ на СЧ ОКР «Амезит-В».

А.35.2 В соответствии с требованиями пунктов 3.2.3, 3.2.3.8 ТЗ на СЧ ОКР «Амезит-В» СПО ПМС должно обеспечивать поиск, выявление на основе ключевых признаков и представление на анализ оператору новых информационных ресурсов для определения необходимости сбора информации.

А.35.3 Для проведения проверки СПО ПМС на соответствие предъявляемым требованиям необходимо выполнить действия, описанные ниже.

А.35.3.1 На рабочем столе АРМ оператора запустить обозреватель.

А.35.3.2 В адресной строке ввести адрес сервера приложений и нажать на клавишу «Enter». Адрес сервера приложений уточняется после установки и настройки СПО ПМС согласно документу RU.BATC.00179-01 32 01 «Специальное программное обеспечение подсистемы мониторинга сети Интернет и СМИ. Руководство системного программиста». Откроется страница авторизации.

А.35.3.3 На странице авторизации ввести аутентификационные данные (логин: operator3, пароль: password) и нажать на кнопку «Войти». Откроется страница со списком источников.

А.35.3.4 На странице со списком источников нажать на кнопку «Поиск источников».

А.35.3.5 В поле «Текст» ввести текст, по которому будет произведен поиск новых источников.

А.35.3.6 Нажать на кнопку «Начать поиск».

А.35.3.7 Подождать, пока списке источников не появятся новые источники (от 1 до 30 минут). У новых источников в столбце «Активен» флаг будет отсутствовать.

А.35.3.8 У нового источника в столбце «Активен» нажать на переключатель, чтобы включить его в процедуру сбора.

А.35.3.9 Выполнить процедуру настроки шаблонов для данного источника согласно документу RU.BATC.00179-01 34 01 «Специальное программное обеспечение подсистемы мониторинга сети Интернет и СМИ. Руководство оператора».

А.35.3.10 В адресной строке ввести адрес сервера приложений и нажать на клавишу «Enter». Адрес сервера приложений уточняется после установки и настройки СПО ПМС согласно документу RU.BATC.00179-01 32 01 «Специальное программное обеспечение подсистемы мониторинга сети Интернет и СМИ. Руководство системного программиста». Откроется страница авторизации.

А.35.3.11 На странице авторизации ввести аутентификационные данные (логин: admin, пароль: password) и нажать на кнопку «Войти». Откроется стартовая страница с отслеживаемыми тематиками. Описание интерфейса СПО ПМС приведено в документе RU.BATC.00179-01 34 01 «Специальное

программное обеспечение подсистемы мониторинга сети Интернет и СМИ. Руководство оператора».

А.35.3.12 На панели фильтров в поле «Источник» выбрать новый источник публикации.

А.35.3.13 Закрыть панель фильтров, нажав на кнопку «Закрыть». Отобразятся публикации из нового источника.

Примечание. Новые публикации появятся при следующем цикле сбора, необходимо подождать от 5 до 30 минут для получения публикаций.

А.35.1 СПО ПМС считается выдержавшим испытания по п. А.35.3.1-А.35.3.13 программы и методики испытаний и выполняющим пункты 3.2.3, 3.2.3.8 ТЗ на СЧ ОКР, если:

- в процессе процедуры настройки параметров поиска не было ошибок;
- в списке источников появился новый источник данных;
- столбце «Активен» у нового источника отсутствует флаг;
- в списке публикаций появились публикации из нового источника.

А.36 Методика № 36

А.36.1 В данной методике проводится проверка СПО ПМС на соответствие требованиям пунктов 3.2.3, 3.2.3.9 ТЗ на СЧ ОКР «Амезит-В».

А.36.2 В соответствии с требованиями пунктов 3.2.3, 3.2.3.9 ТЗ на СЧ ОКР «Амезит-В» СПО ПМС должно обеспечивать автоматизированное составление аналитических справок о различных событиях, объектах и персонах в заданном интервале времени по временным, адресным, региональным параметрам и по источникам их появления.

А.36.2.1 Должны формироваться следующие отчеты:

- отчет по публикациям;
- отчет с хронологией появления публикаций;
- отчет по событиям;
- отчет по персонам.

А.36.2.1.1 В состав отчета по публикациям должны входить следующие данные:

- тематика выборки публикаций;
- количество публикаций по тематике;
- источников публикаций;
- количество публикаций в каждом источнике;
- названия событий, упомянутых в публикациях;
- количество упоминаний событий по тематике;
- количество упоминаний событий в каждом источнике;

- названия персон, упомянутых в публикациях;
- количество упоминаний персон по тематике;
- количество упоминаний персон в каждом источнике;
- заголовки публикаций;
- тексты публикаций;
- даты публикаций;
- источники публикаций;
- авторы публикаций;
- тональность публикации;
- географическое расположение публикаций.

А.36.3 Для проведения проверки СПО ПМС на соответствие предъявляемым требованиям необходимо выполнить действия, описанные ниже.

А.36.3.1 Повторить пункты с А.28.3.1 по А.28.3.4 (Методика № 28).

А.36.3.2 На панели фильтров выбрать:

- в поле «Тематика» – тематику публикаций;
- в поле «Автор» – авторов публикаций;
- в поле «Источник» – источник публикаций;
- в полях «Страна», «Регион» или «Город» – регион публикаций;
- в поле «Дата от» – начальную дату отбора публикаций;
- в поле «Дата до» – конечную дату отбора публикаций.

А.36.3.3 Закрыть панель фильтров, нажав на кнопку «Закрыть». В списке публикаций отобразятся отфильтрованные публикации.

А.36.3.4 В верхней части страницы над списком публикаций нажать на значок печати. Откроется окно «Экспорт файла для печати».

А.36.3.5 В открывшемся окне выполнить следующие действия:

- в поле «Тип файла» выбрать из раскрывающего списка тип выходного файла;
- в поле «Отчет по» выбрать из раскрывающегося списка тип отчета;

А.36.3.6 Нажать на кнопку «Экспорт».

А.36.3.7 Сохранить полученный файл.

А.36.4 СПО ПМС считается выдержавшим испытания по п. А.36.3.1-А.36.3.7 программы и методики испытаний и выполняющим пункты 3.2.3, 3.2.3.9 ТЗ на СЧ ОКР, если:

- файл сформирован в выбранном типе выходного файла;
- в файле содержатся данные, сформированные согласно типу отчета и параметрам фильтрации, а также указанные в п. 3.2.19.9 Дополнения №1 к ТТЗ.

А.37 Методика № 37

А.37.1 В данной методике проводится проверка СПО ПМС на соответствие требованиям пунктов 3.2.3, 3.2.3.10 ТЗ на СЧ ОКР «Амезит-В».

А.37.2 В соответствии с требованиями пунктов 3.2.3, 3.2.3.10 ТЗ на СЧ ОКР «Амезит-В» действия СПО ПМС не должны определяться как элементы инфраструктуры государственных органов.

А.37.3 Для проведения проверки СПО ПМС на соответствие предъявляемым требованиям необходимо выполнить действия, описанные ниже.

А.37.3.1 Выполнить действия по проверке анонимизации действий сборщиков согласно документу RU.ВАТС.00179-01 32 01 «Специальное программное обеспечение подсистемы мониторинга сети Интернет и СМИ. Руководство системного программиста».

А.37.4 СПО ПМС считается выдержавшим испытания по п. А.37.3.1 программы и методики испытаний и выполняющим пункты 3.2.3, 3.2.3.10 ТЗ на СЧ ОКР, если:

- сборщики имеют соединение только с сервисами анонимизации;
- сервисы анонимизации имеют разные адреса выхода в сеть.

А.38 Методика № 38

А.38.1 В данной методике проводится проверка СПО ПМС на соответствие требованиям пунктов 3.2.3, 3.2.3.11 ТЗ на СЧ ОКР «Амезит-В».

А.38.2 В соответствии с требованиями пунктов 3.2.3, 3.2.3.11 ТЗ на СЧ ОКР «Амезит-В» СПО ПМС должно обеспечивать возможность автоматизированного взаимодействия с СПО подсистемы лингвистического обеспечения.

А.38.3 Для проведения проверки СПО ПМС на соответствие предъявляемым требованиям необходимо выполнить действия, описанные ниже.

А.38.3.1 Повторить пункты с А.28.3.1 по А.28.3.2 (Методика № 28).

А.38.3.2 В верхней части страницы нажать на строку поиска. Откроется панель фильтров.

А.38.3.3 В панели фильтров в поле «Источники» выбрать социальную сеть «Twitter».

А.38.3.4 Закрыть панель фильтров, нажав на «Закрыть». В списке публикаций будут отображены публикации из социальной сети Twitter, тексты публикации которых будут отображены на русском языке.

А.38.4 СПО ПМС считается выдержавшим испытания по п. А.38.3.1-А.38.3.4 программы и методики испытаний и выполняющим пункты 3.2.3, 3.2.3.11 ТЗ на СЧ ОКР, если тексты статей из социальной сети Twitter были отображены на русском языке.

А.39 Методика № 39

А.39.1 В данной методике проводится проверка СПО ПМС на соответствие требованиям пунктов 3.2.3, 3.2.3.12 ТЗ на СЧ ОКР «Амезит-В».

А.39.2 В соответствии с требованиями пунктов 3.2.3, 3.2.3.12 ТЗ на СЧ ОКР «Амезит-В» должна быть реализована возможность удаленного использования СПО ПМС территориально распределенными элементами АПК «Амезит» (через подсистему ППД) с разграничением прав доступа согласно ролевой модели доступа, включающей следующие роли:

- администратор;
- оператор-аналитик;
- оператор сбора информации.

А.39.2.1 Роль «Администратор» должна включать следующие возможности:

- управление пользователями ПМС;
- управление всеми тематиками мониторинга;
- мониторинг и аналитика социальных сетей и СМИ сети Интернет;
- управление шаблонами сбора информации;
- управление настройками сбора информации.

А.39.2.2 Роль «Оператор-аналитик» должна включать следующие возможности:

- управление личными тематиками мониторинга;
- мониторинг и аналитика социальных сетей и СМИ сети Интернет;

А.39.2.3 Роль «Оператор сбора информации» должна включать следующие возможности:

- управление шаблонами сбора информации;
- управление настройками сбора информации.

А.39.3 Для проведения проверки СПО ПМС на соответствие предъявляемым требованиям необходимо выполнить действия, описанные ниже.

А.39.3.1 Выполнить пункты с А.28.3.1 по А.28.3.3 (Методика № 28).

А.39.3.2 Выполнить действия по созданию пользователя operator1 (логин: operator1, пароль: password, роль: оператор-аналитик), operator2 (логин: operator2, пароль: password, роль: оператор-аналитик) и operator2 (логин:

operator2, пароль: password, роль: оператор сбора) согласно документу RU.BATC.00179-01 32 01 «Специальное программное обеспечение подсистемы мониторинга сети Интернет и СМИ. Руководство системного программиста».

А.39.3.3 В верхней части страницы нажать на пиктограмму меню.

А.39.3.4 В меню выбрать пункт «Выход». Откроется страница авторизации.

А.39.3.5 На странице авторизации ввести аутентификационные данные (логин: operator1, пароль: password) и нажать на кнопку «Войти». Откроется стартовая страница с отслеживаемыми тематиками.

А.39.3.6 В верхней части страницы нажать на пиктограмму меню.

А.39.3.7 В меню выбрать пункт «Тематики». Откроется страница со списком тематик, по которым происходит сбор информации.

А.39.3.8 Нажать на кнопку «Добавить» для создания новой тематики. Откроется окно создания тематики.

А.39.3.9 В открывшемся окне ввести:

- в поле «Название» – название тематики;
- в поле «Ключевые слова» – список слов или словосочетаний, по которым осуществляется поиск публикаций;
- в поле «Исключающие слова» список слов или словосочетаний, по которым публикации исключаются из сбора.

А.39.3.10 Нажать на кнопку «Сохранить».

А.39.3.11 В верхней части страницы нажать на значок перехода к стартовой странице. Откроется стартовая страница с отслеживаемыми тематиками.

А.39.3.12 В верхней части страницы нажать на пиктограмму меню.

А.39.3.13 В меню выбрать пункт «Выход». Откроется страница авторизации.

А.39.3.14 На странице авторизации ввести аутентификационные данные (логин: operator2, пароль: password) и нажать на кнопку «Войти». Откроется стартовая страница с отслеживаемыми тематиками.

А.39.3.15 В верхней части страницы нажать на пиктограмму меню.

А.39.3.16 В меню выбрать пункт «Тематики». Откроется страница со списком тематик, по которым происходит сбор информации.

А.39.3.17 Нажать на кнопку «Добавить» для создания новой тематики. Откроется окно создания тематики.

А.39.3.18 В открывшемся окне ввести:

- в поле «Название» – название тематики;

- в поле «Ключевые слова» – список слов или словосочетаний, по которым осуществляется поиск публикаций;
- в поле «Исключающие слова» – список слов или словосочетаний, по которым публикации исключаются из сбора.

А.39.3.19 Нажать на кнопку «Сохранить».

А.39.3.20 В верхней части страницы нажать на значок перехода к стартовой странице. Откроется стартовая страница с отслеживаемыми тематиками.

А.39.3.21 В верхней части страницы нажать на пиктограмму меню.

А.39.3.22 В меню выбрать пункт «Выход». Откроется страница авторизации.

А.39.3.23 На странице авторизации ввести аутентификационные данные (логин: operator3, пароль: password) и нажать на кнопку «Войти». Доступ будет запрещен.

А.39.3.24 На странице авторизации ввести аутентификационные данные (логин: admin, пароль: password) и нажать на кнопку «Войти». Открывется стартовая страница с отслеживаемыми тематиками.

А.39.3.25 В верхней части страницы нажать на пиктограмму меню.

А.39.3.26 В меню выбрать пункт «Выход». Откроется страница авторизации

А.39.3.27 В адресной строке ввести адрес сервера, содержащего настройки сборщика, расположенного на сервере сбора информации, и нажать на клавишу «Enter». Адрес сервера, содержащей настройки сборщика, уточняется после установки и настройки СПО ПМС согласно документу RU.ВАТС.00179-01 32 01 «Специальное программное обеспечение подсистемы мониторинга сети Интернет и СМИ. Руководство системного программиста».

А.39.3.28 На странице авторизации ввести аутентификационные данные (логин: operator3, пароль: password) и нажать на кнопку «Войти». Откроется страница со списком источников.

А.39.3.29 В верхней части страницы нажать на пиктограмму меню.

А.39.3.30 В меню выбрать пункт «Выход». Откроется страница авторизации.

А.39.3.31 На странице авторизации ввести аутентификационные данные (логин: admin, пароль: password) и нажать на кнопку «Войти». Откроется страница со списком источников.

А.39.3.32 В верхней части страницы нажать на пиктограмму меню.

А.39.3.33 В меню выбрать пункт «Выход». Откроется страница авторизации.

А.39.3.34 На странице авторизации ввести аутентификационные данные (логин: operator1, пароль: password) и нажать на кнопку «Войти». Доступ будет запрещен.

А.39.4 СПО ПМС считается выдержавшим испытания по п. А.39.3.1-А.39.3.34 программы и методики испытаний и выполняющим пункты 3.2.3, 3.2.3.12 ТЗ на СЧ ОКР, если:

- список отслеживаемых тематик для пользователя operator1 отличается от списка отслеживаемых тематик для пользователя operator2;
- оператор operator3 не имеет доступа к интерфейсу отслеживания тематик;
- operator1 и operator2 не имеют доступа с настройкам сборщиков;
- администратор admin видит отслеживаемые тематики operator1 и operator2;
- администратор admin имеет доступ к настройкам сборщиков.

А.40 Методика № 40

А.40.1 В данной методике проводится проверка СПО ПОТ на соответствие требованиям пунктов 3.2.4, 3.2.4.1 ТЗ на СЧ ОКР «Амезит-В».

А.40.2 В соответствии с требованиями пунктов 3.2.4, 3.2.4.1 ТЗ на СЧ ОКР «Амезит-В» СПО ПОТ должно обеспечивать тестирование телекоммуникационного оборудования уровня распределения и уровня ядра на возможность проникновения внешнего нарушителя и возможность установки сторонних модулей расширения с применением следующих подходов:

- определение в автоматизированном режиме сетевых настроек (IP-адрес, маска подсети) при подключении к сегменту сети для осуществления поиска и сканирования телекоммуникационного оборудования и систем жизнеобеспечения;
- автоматизированный поиск телекоммуникационного оборудования и систем жизнеобеспечения;
- определение в автоматизированном режиме открытых транспортных портов на телекоммуникационном оборудовании и системах жизнеобеспечения;
- определение в автоматизированном режиме данных о производителе, модели устройства и версии операционной системы телекоммуникационного оборудования и систем жизнеобеспечения;
- подбор паролей по словарю в автоматизированном режиме к сервисам администрирования телекоммуникационного оборудования и систем жизнеобеспечения (с возможностью управления числом и таймаутом задач);

- автоматизированный поиск уязвимостей для идентифицированной версии программного обеспечения телекоммуникационного оборудования и систем жизнеобеспечения по встроенной базе уязвимостей (при этом должна быть предусмотрена процедура обновления встроенной базы уязвимостей);

- установку модулей расширения в виде командных сценариев при наличии административного доступа к управлению устройством.

Примечания:

1. Должно быть предусмотрено решение по противодействию обнаружения попыток перебора паролей системами защиты информации (в том числе, встроенными).

2. Процедура обновления базы уязвимостей должна быть автоматизирована.

А.40.3 Проверка выполняется в соответствии с пунктами А.40.4-А.40.14.1.

А.40.4 Для проверки определения в автоматизированном режиме сетевых настроек (IP-адрес, маска подсети) при подключении к сегменту сети для осуществления поиска и сканирования телекоммуникационного оборудования и систем жизнеобеспечения необходимо произвести проверку возможности определения в автоматизированном режиме сетевых настроек при подключении к сегменту сети с поддержкой протокола DHCP, выполнив следующие действия, описанные ниже.

А.40.4.1 Собрать стенд в соответствии со схемой (см. рисунок Рисунок 2). Запустить dhcp-сервер, входящий в состав коммутационного оборудования стенда, либо на узле DD-WRT в виде сервиса с назначением диапазона адресов 10.0.6.10-250.

А.40.4.2 На АРМ ПОТ запустить СПО ПОТ: «#pot».

А.40.4.3 Выбрать пункт меню: «File» → «Connection manager».

А.40.4.4 В диалоговом окне способов подключения к сети выбрать пункт «DHCP client» и нажать на кнопку «Next».

А.40.4.5 В появившемся диалоговом окне нажать на кнопку «Start» и дождаться появления значения в поле «IP found».

А.40.4.6 В отдельном окне консоли набрать команду: «#ifconfig».

А.40.4.7 В отдельном окне консоли выполнить команду (указав IP-адрес узла DD-WRT):

```
ping -c4 10.0.6.207
```

А.40.4.8 Проверка в соответствии с пунктами А.40.4-А.40.4.7 считается выполненной успешно, если:

- значения параметров сетевых интерфейсов, отображенные в консоли, совпадают со значениями в интерфейсе менеджера подключений;

- полученные значения параметров в интерфейсе менеджера подключений соответствуют значениям параметров IP-адресов, указанных в схеме стенда;

- в окне консоли АРМ ПОТ отобразилась информация о доступности узла следующего вида:

```
PING 10.0.6.207 (10.0.6.207) 56(84) bytes of data.
64 bytes from 10.0.6.207: icmp_seq=1 ttl=255 time=17.9 ms
64 bytes from 10.0.6.207: icmp_seq=2 ttl=255 time=2.27 ms
64 bytes from 10.0.6.207: icmp_seq=3 ttl=255 time=1.13 ms
64 bytes from 10.0.6.207: icmp_seq=4 ttl=255 time=1.19 ms
--- 10.0.6.207 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3004ms
rtt min/avg/max/mdev = 1.137/5.651/17.998/7.142 ms
```

А.40.5 Для проверки определения в автоматизированном режиме сетевых настроек (IP-адрес, маска подсети) при подключении к сегменту сети для осуществления поиска и сканирования телекоммуникационного оборудования и систем жизнеобеспечения необходимо произвести проверку возможности определения в автоматизированном режиме сетевых настроек при подключении к сегменту сети со статическими настройками, выполнив следующие действия, описанные ниже.

А.40.5.1 Собрать стенд в соответствии со схемой (см. рисунок Рисунок 2).

А.40.5.2 Отключить службу DHCP тестового контура (на коммутационном оборудовании или узле DD-WRT).

А.40.5.3 На АРМ ПОТ запустить СПО ПОТ, выполнив в окне консоли команду: «#pot».

А.40.5.4 Выбрать пункт меню: «File» → «Connection manager».

А.40.5.5 В диалоговом окне способов подключения к сети выбрать пункт «Manually» и нажать на кнопку «Next».

А.40.5.6 Выбрать значение сетевого интерфейса «Interface» – «eth0».

А.40.5.7 Указать значения ip= «10.0.6.50», mask= «255.255.255.0», MAC-адрес оставить без изменений.

А.40.5.8 Нажать на кнопку «Connect».

А.40.5.9 В окне консоли АРМ ПОТ набрать команду (указав IP-адрес узла DD-WRT): «ping -c4 10.0.6.207».

А.40.5.10 Включить службу DHCP тестового контура (на коммутационном оборудовании или узле DD-WRT).

А.40.5.11 Проверка в соответствии с пунктами А.40.5.1-А.40.5.10 считается выполненной успешно, если в окне консоли АРМ ПОТ отобразилась информация о доступности сервера DHCP следующего вида:

```
PING 10.0.6.207 (10.0.6.207) 56(84) bytes of data.
64 bytes from 10.0.6.207: icmp_seq=1 ttl=255 time=17.9 ms
64 bytes from 10.0.6.207: icmp_seq=2 ttl=255 time=2.27 ms
64 bytes from 10.0.6.207: icmp_seq=3 ttl=255 time=1.13 ms
64 bytes from 10.0.6.207: icmp_seq=4 ttl=255 time=1.19 ms
--- 10.0.6.207 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3004ms
rtt min/avg/max/mdev = 1.137/5.651/17.998/7.142 ms
```

А.40.6 Для проверки определения в автоматизированном режиме сетевых настроек (IP-адрес, маска подсети) при подключении к сегменту сети для осуществления поиска и сканирования телекоммуникационного оборудования и систем жизнеобеспечения необходимо произвести проверку возможности определения в автоматизированном режиме сетевых настроек при подключении к сегменту сети, выполнив следующие действия, описанные ниже.

А.40.6.1 Собрать стенд в соответствии со схемой (см. рисунок Рисунок 2). Запустить dhcp сервер, входящий в состав коммутационного оборудования стенда, либо на узле DD-WRT в виде сервиса с назначением диапазона адресов 10.0.6.10-250.

А.40.6.2 На АРМ ПОТ запустить СПО ПОТ, выполнив в окне консоли команду: «#pot».

А.40.6.3 Выбрать пункт меню: «File» → «Connection manager».

А.40.6.4 В диалоговом окне способов подключения к сети выбрать пункт «Automatically» и нажать на кнопку «Next».

А.40.6.5 Выбрать значение сетевого интерфейса «Interface» – «eth0».

А.40.6.6 Нажать на кнопку «Search».

А.40.6.7 Дождаться обнаружения трех значений (процесс обнаружения при этом завершится автоматически).

А.40.6.8 Выбрать одно из найденных значений и нажать на кнопку «Next».

А.40.6.9 В появившемся окне оставить без изменений поля ввода и нажать на кнопку «Connect».

А.40.6.10 В отдельной окне консоли выполнить команду (указав IP-адрес узла DD-WRT): «ping -c4 10.0.6.207».

А.40.6.11 Проверка в соответствии с пунктами А.40.6-А.40.6.10 считается выполненной успешно, если в окне консоли АРМ ПОТ отобразилась информация о доступности узла следующего вида:

```
PING 10.0.6.207 (10.0.6.207) 56(84) bytes of data.
64 bytes from 10.0.6.207: icmp_seq=1 ttl=255 time=17.9 ms
64 bytes from 10.0.6.207: icmp_seq=2 ttl=255 time=2.27 ms
64 bytes from 10.0.6.207: icmp_seq=3 ttl=255 time=1.13 ms
64 bytes from 10.0.6.207: icmp_seq=4 ttl=255 time=1.19 ms
--- 10.0.6.207 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3004ms
rtt min/avg/max/mdev = 1.137/5.651/17.998/7.142 ms
```

А.40.7 Для проверки возможности автоматизированного поиска телекоммуникационного оборудования и системах жизнеобеспечения необходимо выполнить следующие действия, описанные ниже.

А.40.7.1 Собрать стенд в соответствии со схемой (см. рисунок Рисунок 2).

А.40.7.2 На АРМ ПОТ в отдельном терминале из директории дистрибутива СПО ПОТ запустить утилиту генерации тестового трафика АСУ ТП: «#./test/trafficGenerator».

А.40.7.3 На АРМ ПОТ запустить СПО ПОТ, выполнив в окне консоли команду: «#pot».

А.40.7.4 На панели управления нажать на кнопку «Run».

А.40.7.5 В появившемся диалоговом окне поле «Scan group name» оставить без изменений, режим сканирования «Scan type» установить в режиме «Active».

А.40.7.6 Выбрать сетевой интерфейс «Network interface» – «eth0».

А.40.7.7 Выбрать пункт «Common».

А.40.7.8 Задать «Risk level: Low».

А.40.7.9 Указать значение «Subnet»: указать IP-адрес сети в соответствии со схемой стенда для сегмента сети к которому осуществляется подключение.

А.40.7.10 Нажать на кнопку «Start» и дождаться сообщения о завершении сканирования.

А.40.7.11 В сформированном дереве узлов выполнить переключение между элементами.

А.40.7.12 Проверка в соответствии с пунктами А.40.7-А.40.7.11 считается выполненной успешно, если можно выполнить переключение между элементами дерева узлов и просмотреть следующую информацию:

- список элементов дерева узлов;
- список найденных уязвимостях;
- версия операционной системы;
- список обнаруженных сервисов.

А.40.8 Для проверки возможности определения в автоматизированном режиме открытых транспортных портов на телекоммуникационном оборудовании и системах жизнеобеспечения необходимо выполнить следующие действия, описанные ниже.

А.40.8.1 Собрать стенд в соответствии со схемой (см. рисунок Рисунок 2).

А.40.8.2 На АРМ ПОТ в отдельном терминале из директории дистрибутива СПО ПОТ запустить утилиту генерации тестового трафика АСУ ТП, выполнив команду: «#./test/trafficGenerator».

А.40.8.3 На АРМ ПОТ запустить СПО ПОТ, выполнив в окне консоли команду: «#pot».

А.40.8.4 На панели управления нажать на кнопку «Run».

А.40.8.5 В появившемся диалоговом окне поле «Scan group name» оставить без изменений, режим сканирования «Scan type» установить в режиме «Active».

А.40.8.6 Выбрать сетевой интерфейс «Network interface» – «eth0».

А.40.8.7 Выбрать пункт «Common».

А.40.8.8 Задать «Risk level: Low».

А.40.8.9 Указать значение «Subnet»: указать IP-адрес сети в соответствии со схемой стенда для сегмента сети к которому осуществляется подключение.

А.40.8.10 Нажать на кнопку «Start» и дождаться сообщения о завершении сканирования.

А.40.8.11 В сформированном списке узлов выбрать «DVL».

А.40.8.12 В раскрывшемся списке портов последовательно выбрать несколько элементов.

А.40.8.13 Проверка в соответствии с пунктами А.40.8.1-А.40.8.12 считается выполненной успешно, если в интерфейсе отобразилась информация о выбранных портах.

А.40.9 Для проверки возможности определения в автоматизированном режиме сведений о производителе, модели устройства и версии операционной системы телекоммуникационного оборудования и систем жизнеобеспечения необходимо выполнить следующие действия, описанные ниже.

А.40.9.1 На АРМ ПОТ в отдельном терминале из директории дистрибутива СПО ПОТ запустить утилиту генерации тестового трафика АСУ ТП, выполнив команду: «#./test/trafficGenerator».

А.40.9.2 На АРМ ПОТ запустить СПО ПОТ, выполнив в окне консоли команду: «#pot».

А.40.9.3 На панели управления нажать на кнопку «Run».

А.40.9.4 В появившемся диалоговом окне поле «Scan group name» оставить без изменений, режим сканирования «Scan type» установить в режиме «Active».

А.40.9.5 Выбрать сетевой интерфейс «Network interface» – «eth0».

А.40.9.6 Выбрать пункт «Common».

А.40.9.7 Задать «Risk level».

А.40.9.8 Указать значение «Subnet»: указать IP-адрес сети в соответствии со схемой стенда для сегмента сети к которому осуществляется подключение.

А.40.9.9 Нажать на кнопку «Start» и дождаться сообщения о завершении сканирования.

А.40.9.10 В сформированном дереве узлов выполнить переключение между элементами. Убедиться, что есть возможность посмотреть информацию о элементах дерева узлов. Примечание: наличие иконки в виде «шестеренки» – узел относится к классу промышленных систем управления технологическим процессом.

А.40.9.11 Выбрать несколько произвольных узлов различного типа.

А.40.9.12 Проверка в соответствии с пунктами А.40.9.1-А.40.9.11 считается выполненной успешно, если в интерфейсе отобразилась информация о производителе, модели устройства и версии операционной системы при выборе найденных узлов сети.

А.40.10 Для проверки возможности подбора паролей по словарю в автоматизированном режиме к сервисам администрирования телекоммуникационного оборудования и систем жизнеобеспечения (с возможностью управления числом и таймаутом задач, в том числе путем выбора этих параметров из списка рекомендованных значений для отдельных категорий устройств) необходимо выполнить следующие действия, описанные ниже.

А.40.10.1 Предварительно открыть файл ./pot/etc/500-worst-passwords.txt и добавить в произвольном месте строку «admin». Запустить на узле DD-WRT ssh сервер на 22 порту (sudo service sshd restart) с добавленным пользователем/паролем root:admin.

А.40.10.2 Собрать стенд в соответствии со схемой (см. рисунок Рисунок 2).

А.40.10.3 На АРМ ПОТ запустить СПО ПОТ, выполнив в окне консоли команду: «#pot».

А.40.10.4 На панели управления нажать на кнопку «Run».

А.40.10.5 В открывшемся диалоговом окне поле «Scan group name» оставить без изменений, режим сканирования «Scan type» установить в «Active».

А.40.10.6 Выбрать сетевой интерфейс «Network interface» – «eth0».

А.40.10.7 Выбрать пункт «Common».

А.40.10.8 Задать «Risk level: Medium».

А.40.10.9 Указать «Subnet»: указать IP-адрес сети в соответствии со схемой стенда для сегмента сети, к которому осуществляется подключение.

А.40.10.10 Нажать на кнопку «Start» и дождаться сообщения о завершении сканирования.

А.40.10.11 Выбрать узел «DD-WRT».

А.40.10.12 Правой кнопкой мыши нажать на имя данного сервиса и в контекстном меню выбрать пункт «Password brute-force».

А.40.10.13 В открывшемся диалоговом окне установить следующие параметры:

- «Host»: 10.0.6.207; (указать IP-адрес узла DD-WRT)
- «Port»: 22;
- «Service»: ssh;
- «Login»: root;
- «Password» (выбрать ниже From file): указать ./pot/etc/500-worst-passwords.txt;

А.40.10.14 Остальные поля оставить без изменений и нажать на кнопку «Start».

А.40.10.15 Проверка в соответствии с пунктами А.40.10.1-А.40.10.14 считается выполненной успешно, если появилось окно, содержащее оповещение «Found a password for service ssh!».

А.40.11 Для проверки отсутствия возможности выявления попыток перебора паролей современными системами защиты информации (в том числе встроенными) необходимо выполнить следующие действия, описанные ниже.

А.40.11.1 Перейти на узел Bruteforce detector в соответствии со схемой стенда (см. рисунок Рисунок 2). Скопировать архив утилиты Brute Force Detection из директории «distrib/test» в домашнюю директорию: «/usr/local/src».

А.40.11.2 Разархивировать программу «tar -xzvf bfd-*.tar.gz».

А.40.11.3 Перейти в директорию с программой «cd bfd-*».

А.40.11.4 Установить «./install.sh».

А.40.11.5 Выполнить установку сервера SSH: «sudo apt-get install ssh».

А.40.11.6 Добавить в файл «/etc/ssh/sshd_config» строку «PermitRootLogin yes» и сохранить.

А.40.11.7 Установить пароль для пользователя «root:toor», выполнив команду: «passwd root».

А.40.11.8 Выполнить команду: «sudo service sshd restart».

А.40.11.9 Выполнить команду «bfd -s» и внести задачу в cron с интервалом проверки 1 минута.

А.40.11.10 На АРМ ПОТ запустить СПО ПОТ, выполнив команду: «#pot».

А.40.11.11 Нажать на кнопку «Run» (серый треугольник в панели управления).

А.40.11.12 В появившемся диалоговом окне поле «Scan group name» оставить без изменений, для режима сканирования «Scan type» установить значение «Active».

А.40.11.13 Выбрать сетевой интерфейс «Network interface» – «eth0».

А.40.11.14 Выбрать пункт «Common» (режим типового сканирования).

А.40.11.15 Задать «Risk level: Medium».

А.40.11.16 Указать «Subnet»: 10.0.6.206 (указать IP-адрес узла DVL).

А.40.11.17 Нажать на кнопку «Start» и дождаться сообщения о завершении сканирования.

А.40.11.18 Выбрать узел 10.0.6.31 (указать IP-адрес узла Bruteforce detector) и в списке портов выбрать сервис ssh/22.

А.40.11.19 Нажать правой кнопкой мыши на имя данного сервиса и в контекстном меню выбрать пункт «Password brute-force».

А.40.11.20 В появившемся диалоговом окне установить следующие параметры:

- Host: 10.0.6.31 (указать IP-адрес узла Bruteforce detector);
- Port: 22;
- Service: ssh;
- Login: root;
- Password (выбрать ниже From file): указать «./pot/etc/500-worst-passwords.txt».

А.40.11.21 Установить для параметра «Wait time» значение «2».

А.40.11.22 Остальные поля оставить без изменений и нажать на кнопку «Start».

А.40.11.23 Дождаться появления окна с оповещением «Found a password for service ssh!».

А.40.11.24 Перейти на узел Bruteforce detector.

А.40.11.25 Выполнить команду: «bfd -a».

А.40.11.26 Проверка в соответствии с пунктами А.40.11.1-А.40.11.25 считается выполненной успешно, если:

- будет отображено сообщение «Found a password for service ssh!»;
- при выборе пункта «Authentication» для узла Bruteforce detector отображается значение данного пароля»;
- команда выдаст следующее содержимое (список атакующих узлов будет пуст):

```
Brute Force Detection v1.5-2 <bfd@r-fx.org>
(C) 1999-2014, R-fx Networks <proj@r-fx.org>
(C) 2014, Ryan MacDonald <ryan@r-fx.org>
This program may be freely redistributed under the terms of the GNU GPL
[+] Top 25 brute force attackers today
#TRIGS  IP  FIRST_SEEN  LAST_SEEN  RULES
[+] Top 25 brute force attackers this week
#TRIGS  IP  FIRST_SEEN  LAST_SEEN  RULES
```

А.40.12 Для проверки возможности автоматизированного поиска уязвимостей для идентифицированной версии программного обеспечения телекоммуникационного оборудования и систем жизнеобеспечения по встроенной базе уязвимостей (при этом должна быть предусмотрена процедура обновления встроенной базы уязвимостей) необходимо выполнить следующие действия, описанные ниже.

А.40.12.1 Собрать стенд в соответствии со схемой (см. рисунок Рисунок 2).

А.40.12.2 Подготовить файл обновления базы уязвимостей allitems-cvrf-year-2018.xml в соответствии с эксплуатационной документацией на СПО ПОТ.

А.40.12.3 Выполнить обновление базы уязвимостей из файла allitems-cvrf-year-2018.xml в соответствии с эксплуатационной документацией на СПО ПОТ.

А.40.12.4 На АРМ ПОТ запустить СПО ПОТ, выполнив в окне консоли команду: «#pot».

А.40.12.5 Выбрать пункт меню «File» → «Vulnerability database search».

А.40.12.6 Ввести ключевое слово «Windows» и нажать на кнопку в виде увеличительного стекла.

А.40.12.7 Проверка в соответствии с пунктами А.40.12.1-А.40.12.6 считается выполненной успешно, если в интерфейсе отобразились результаты поиска по базе уязвимостей.

А.40.13 Для проверки возможности обновления встроенной базы уязвимостей выполните действия, описанные ниже.

А.40.13.1 Собрать стенд в соответствии со схемой (см. рисунок Рисунок 2).

А.40.13.2 Подготовить файл обновления базы уязвимостей allitems-cvrf-year-2018.xml в соответствии с эксплуатационной документацией на СПО ПОТ.

А.40.13.3 На АРМ ПОТ выполнить переустановку базы данных (в целях очистки), выполнив команду: «./install.sh».

А.40.13.4 На АРМ ПОТ запустить СПО ПОТ, выполнив в окне консоли команду: «#pot».

А.40.13.5 Выбрать пункт меню «File» → «Vulnerability database search».

А.40.13.6 Ввести ключевое слово «Windows» и нажать на кнопку в виде увеличительного стекла. Убедиться в отсутствии результатов поиска.

А.40.13.7 Выбрать пункт меню «File» → «Vulnerability database update».

А.40.13.8 Выбрать пункт «From file» и нажать на кнопку «Update».

А.40.13.9 В диалоговом окне выбрать файл allitems-cvrf-year-2018.xml.

А.40.13.10 Дождаться завершения процесса обновления.

А.40.13.11 Выбрать пункт меню «File» → «Vulnerability database search».

А.40.13.12 Ввести ключевое слово «Windows» и нажать на кнопку в виде увеличительного стекла. Убедиться в наличии результатов поиска.

А.40.13.13 Проверка в соответствии с пунктами А.40.13.1-А.40.13.12 считается выполненной успешно, если:

- отсутствуют результаты поиска по ключевому слову в пункте А.40.13.6;
- присутствуют результаты поиска по ключевому слову в пункте А.40.13.12.

А.40.14 Для проверки установки модулей расширения в виде командных сценариев при наличии административного доступа к управлению устройством выполните действия, описанные ниже.

А.40.14.1 Выполнить командные сценарии по нарушению функционирования сетевых устройств производства Cisco, Juniper и Huawei в соответствии с документом RU.BATC.00180 -01 31 01 «Специальное программное обеспечение подсистемы анализа информационно-технических объектов телекоммуникационных систем. Описание применения» Приложения 1.

А.40.14.2 Проверка в соответствии с пунктами А.40.14-А.40.14.1 считается выполненной успешно, если при выполнении командных сценариев произошла установка модулей расширения.

А.40.15 СПО ПОТ считается выдержавшим испытания по пунктам А.40.4-А.40.14.2 программы и методики испытаний и выполняющим пункты 3.2.4, 3.2.4.1 ТЗ на СЧ ОКР «Амезит-В», если успешно завершены проверки пунктов А.40.4.8, А.40.5.11, А.40.6.11, А.40.7.12, А.40.8.13, А.40.9.12, А.40.10.15, А.40.11.26, А.40.12.7, А.40.13.13, А.40.14.2.

А.41 Методика № 41

А.41.1 В данной методике проводится проверка СПО ПОТ на соответствие требованиям пунктов 3.2.4, 3.2.4.2 ТЗ на СЧ ОКР «Амезит-В».

А.41.2 В соответствии с требованиями пунктов 3.2.4, 3.2.4.2 ТЗ на СЧ ОКР «Амезит-В» СПО ПОТ должно обеспечивать проведение нагрузочного и функционального тестирования, направленных на блокирование работы телекоммуникационного оборудования, с реализацией следующих требований:

- генерировать характерные для конкретных корпоративных или операторских сетей комбинации трафика на скорости не менее 40 Гбит/с;
- обеспечивать возможность подключения к сети по технологиям Ethernet и Fiber Optic;
- обеспечивать возможность загрузки образцов сетевого трафика для использования его в качестве нагрузки при тестировании;
- предоставлять возможность модификации записанного трафика DoS-атаки для организации переадресации этого трафика на тестируемый узел.

А.41.3 Проверка выполняется в соответствии с пунктами А.41.4-А.41.8.13.

А.41.4 Для проведения проверки возможности генерации характерных для конкретных корпоративных или операторских сетей комбинаций трафика на скорости не менее 40 Гбит/с необходимо выполнить следующие действия, описанные ниже.

А.41.4.1 Собрать стенд в соответствии со схемой (см. рисунок Рисунок 2).

А.41.4.2 На АРМ ПОТ запустить СПО ПОТ, выполнив в окне консоли команду: «#pot».

А.41.4.3 Выбрать пункт меню управления генерацией трафика «File» → «Traffic generator».

А.41.4.4 В поле «Source: IP range» ввести значение: 8.8.8.1 / 8.8.8.255.

А.41.4.5 В поле «Destination: IP range» ввести значение: 10.0.6.1 / 10.0.6.255.

А.41.4.6 Нажать на кнопку «Start».

А.41.4.7 Проверка в соответствии с пунктами А.41.4.1-А.41.4.6 считается выполненной успешно, если:

- на панели «Packets» есть возможность просмотреть пакеты генерируемого трафика;
- на панели «Statistics» отображается статистика текущего сеанса;

- скорость генерации пакетов в панели статистики (строка «Gb/s :») составляет не менее 39 (с учетом эффективной пропускной способности канала).

А.41.5 Для проверки возможности подключения к сети по технологии Ethernet необходимо выполнить следующие действия, описанные ниже.

А.41.5.1 Собрать стенд в соответствии со схемой (см. рисунок Рисунок 2).

А.41.5.2 Выполнить подключение АПК СКАТ «Генератор трафика» и АРМ ПОТ к коммутатору, использую Ethernet кабель. Подключение АПК СКАТ «Генератор трафика» выполнить в соответствии с эксплуатационной документацией на данный АПК.

А.41.5.3 На АРМ ПОТ запустить СПО ПОТ, выполнив в окне консоли команду: «#pot».

А.41.5.4 Выбрать пункт меню управления генерацией трафика «File» → «Traffic generator».

А.41.5.5 В соответствии с программной документацией на АПК СКАТ «Генератор трафика» с АРМ ПОТ выполнить подключение по протоколу ssh к АПК СКАТ «Генератор трафика».

А.41.5.6 Выполнить команду ping, с указанием адреса назначения – IP-адреса узла DVL, назначенного в соответствии с конфигурацией стенда.

А.41.5.7 Проверка в соответствии с пунктами А.41.5.1-А.41.5.7 считается выполненной успешно, если:

- в консоли АПК СКАТ Генератор трафик отобразилась информация о доступности узла DVL;
- в СПО ПОТ отобразился интерфейс управления генерацией трафика.

А.41.6 Для проверки возможности подключения к сети по технологии Fiber Optic необходимо выполнить следующие действия, описанные ниже.

А.41.6.1 Собрать стенд в соответствии со схемой (см. рисунок Рисунок 2).

А.41.6.2 Выполнить подключение АПК СКАТ «Генератор трафика» и АРМ ПОТ к коммутатору, используя SFP-модуль и оптоволоконный кабель. Подключение АПК СКАТ «Генератор трафика» выполнить в соответствии с эксплуатационной документацией на данный АПК. Подключение АРМ ПОТ выполнить с использованием медиаконвертера.

А.41.6.3 На АРМ ПОТ запустить СПО ПОТ, выполнив в окне консоли команду: «#pot».

А.41.6.4 Выбрать пункт меню управления генерацией трафика «File» → «Traffic generator».

А.41.6.5 В соответствии с программной документацией на АПК СКАТ «Генератор трафика» с АРМ ПОТ выполнить подключение по протоколу ssh к АПК СКАТ «Генератор трафика».

А.41.6.6 Выполнить команду ping, с указанием адреса назначения – IP-адреса узла DVL, назначенного в соответствии с конфигурацией стенда.

А.41.6.7 Проверка в соответствии с пунктами А.41.6.1-А.41.6.6 считается выполненной успешно, если:

- в консоли АПК СКАТ Генератор трафик отобразилась информация о доступности узла DVL;
- в СПО ПОТ отобразился интерфейс управления генерацией трафика.

А.41.7 Для проведения проверки возможности загрузки образцов сетевого трафика для использования его в качестве нагрузки при тестировании необходимо выполнить следующие действия, описанные ниже.

А.41.7.1 Собрать стенд в соответствии со схемой (см. рисунок Рисунок 2).

А.41.7.2 На АРМ ПОТ запустить СПО ПОТ, выполнив в окне консоли команду: «#pot». В настройках программы указать параметры подключения к АПК «СКАТ. Генератор трафика» в соответствии со спецификацией стенда.

А.41.7.3 Выбрать пункт меню загрузки образцов сетевого трафика «File» → «Upload traffic».

А.41.7.4 В диалоговом окне выбрать (нажав «...») тестовый pcap-файл, предоставляемый в комплекте с АПК «СКАТ. Генератор трафика».

А.41.7.5 Нажать на кнопку «Upload» и дождаться завершения процесса загрузки.

А.41.7.6 Закрыть диалоговое окно.

А.41.7.7 Выбрать пункт меню управления генерацией трафика «File->Traffic generator».

А.41.7.8 Нажать на кнопку «Load pcap dump from file».

А.41.7.9 Выбрать загруженный в память устройства pcap-файл.

А.41.7.10 Нажать на кнопку «Start».

А.41.7.11 Проверка в соответствии с пунктами А.41.7.1-А.41.7.10 считается выполненной успешно, если:

- в панели «Packets» отобразились пакеты генерируемого трафика;
- в панели «Statistics» отобразилась статистика текущего сеанса.

А.41.8 Для проверки возможности модификации записанного трафика DoS-атаки для организации переадресации этого трафика на тестируемый узел необходимо выполнить следующие действия, описанные ниже.

А.41.8.1 Собрать стенд в соответствии со схемой (см. рисунок Рисунок 2).

А.41.8.2 На АРМ ПОТ запустить СПО ПОТ, выполнив в окне консоли команду: «#pot». В настройках программы указать параметры подключения к АПК «СКАТ. Генератор трафика» в соответствии со спецификацией стенда.

А.41.8.3 Выбрать пункт меню загрузки образцов сетевого трафика «File» → «Upload traffic».

А.41.8.4 В диалоговом окне выбрать (нажав «...») тестовый pcap файл, предоставляемый в комплекте с АПК «СКАТ. Генератор трафика».

А.41.8.5 Нажать на кнопку «Upload» и дождаться завершения процесса загрузки.

А.41.8.6 Закрыть диалоговое окно.

А.41.8.7 Выбрать пункт меню управления генерацией трафика «File» → «Traffic generator».

А.41.8.8 Нажать на кнопку «Load pcap dump from file».

А.41.8.9 Выбрать загруженный в память устройства pcap файл.

А.41.8.10 В поле «Source: IP range» ввести: 8.8.8.1 / 8.8.8.255.

А.41.8.11 В поле «Destination: IP range» ввести: 10.0.6.1 / 10.0.6.255.

А.41.8.12 Нажать на кнопку «Start».

А.41.8.13 Проверка в соответствии с пунктами А.41.8.1-А.41.8.12 считается выполненной успешно, если:

- в панели «Packets» отобразились пакеты генерируемого трафика;
- в панели «Statistics» отобразилась статистика текущего сеанса.

А.41.9 СПО ПОТ считается выдержавшим испытания по п. А.41.4-А.41.8.13 программы и методики испытаний и выполняющим пункты 3.2.4, 3.2.4.2 ТЗ на СЧ ОКР, если успешно завершены проверки пунктов А.41.4.7, А.41.5.7, А.41.6.7, А.41.7.11, А.41.8.13.

А.42 Методика № 42

А.42.1 В данной методике проводится проверка СПО ПОТ на соответствие требованиям пунктов 3.2.4, 3.2.4.3 ТЗ на СЧ ОКР «Амезит-В».

А.42.2 В соответствии с требованиями пунктов 3.2.4, 3.2.4.3 ТЗ на СЧ ОКР «Амезит-В» должен быть создан и изготовлен стенд контроля информационно-технических объектов систем жизнеобеспечения с возможностью визуализации механизмов проведения воздействий в составе:

- пусковой комплекс №1 – стенд контроля железнодорожной АСУ ТП.
- пусковой комплекс № 2 – стенд контроля АСУ ТП систем жизнеобеспечения населенного пункта и производства.

Примечания:

1. Стенды должны обеспечивать наглядное отображение на моделях в масштабе не менее 1:70 и 1:87 (стенд № 1 и стенд № 2 соответственно) особенности автоматизации в предметных сферах.

2. В состав стендов должны входить типовые для моделируемых сфер датчики, исполнительные устройства, должны моделироваться типовые технологические процессы.

3. Стенды должны обеспечивать моделирование атак типа ARP-spoofing, приводящих к нарушениям моделируемых технологических процессов.

4. Нарушение моделируемых технологических процессов должно сопровождаться наглядными изменениями в работе макетов (срабатывание световой сигнализации, столкновение объектов, выделение дыма и т.п.).

А.42.3 Проверка выполняется в соответствии с пунктами А.42.4-А.42.10.4.

А.42.4 Для проверки пускового комплекса № 1 на обеспечение наглядного отображения на моделях в масштабе не менее 1:70 и 1:87 (стенд № 1 и стенд № 2 соответственно) особенности автоматизации в предметных сферах необходимо выполнить действия, описанные ниже.

А.42.4.1 Собрать стенд в соответствии со схемой (см. рисунок Рисунок 2).

А.42.4.2 На АРМ оператора АСУ ТП запустить программу ProgS_PLC в соответствии с RU.BATC.00180-01 92 02 «Специальное программное обеспечение подсистемы анализа информационно-технических объектов телекоммуникационных систем. Пусковой комплекс № 1. Стенд контроля железнодорожной АСУ ТП. Руководство пользователя».

А.42.4.3 В соответствии с RU.BATC.00180-01 92 02 «Специальное программное обеспечение подсистемы анализа информационно-технических объектов телекоммуникационных систем. Пусковой комплекс № 1. Стенд контроля железнодорожной АСУ ТП. Руководство пользователя» в интерфейсе пользователя выполнить управление технологическими процессами:

- изменить скорость движения поездов на различных участках железной дороги;
- проверить индикацию состояния объектов инфраструктуры;
- опустить шлагбаумов при приближении поездов;
- проверить работу освещения в домах и на улице;
- проверить индикацию работы ТЭЦ.

А.42.4.4 Проверка в соответствии с пунктами А.42.4-А.42.4.3 считается выполненной успешно, если в результате управления технологическими процессами в интерфейсе пользователя пускового комплекса № 1 особенности автоматизации в предметных сферах отображаются в масштабе не менее 1:70 и 1:87.

А.42.4.5 Для проверки пускового комплекса № 2 на обеспечение наглядного отображения на моделях в масштабе не менее 1:70 и 1:87 (стенд № 1 и стенд №2 соответственно) особенности автоматизации в предметных сферах необходимо выполнить действия, описанные ниже.

А.42.4.6 Собрать стенд в соответствии со схемой (см. рисунок Рисунок 2).

А.42.4.7 На АРМ оператора АСУ ТП запустить программу ProgS_PLC в соответствии с RU.BATC.00180-01 92 03 «Специальное программное обеспечение подсистемы анализа информационно-технических объектов телекоммуникационных систем. Пусковой комплекс № 2. Стенд контроля АСУ ТП систем жизнеобеспечения населенного пункта и производства. Руководство пользователя».

А.42.4.8 В соответствии с RU.BATC.00180-01 92 03 «Специальное программное обеспечение подсистемы анализа информационно-технических объектов телекоммуникационных систем. Пусковой комплекс № 2. Стенд контроля АСУ ТП систем жизнеобеспечения населенного пункта и производства. Руководство пользователя» в интерфейсе пользователя выполнить управление технологическими процессами:

- выполнить имитацию протекания нефтепродуктов по нефтепроводу, путем перекачивания жидкости темного цвета;
- проверить индикацию уровня жидкостей в баках;
- проверить индикацию работы насосного агрегата путем вращения лопастей;
- проверить индикацию состояния (вкл./выкл.).

А.42.4.9 Проверка в соответствии с пунктами А.42.4.5-А.42.4.8 считается выполненной успешно, если в результате управления технологическими процессами в интерфейсе пользователя пускового комплекса № 2 особенности автоматизации в предметных сферах отображается в масштабе не менее 1:70 и 1:87.

А.42.5 Для проверки состава и работы пускового комплекса № 1 необходимо выполнить действия, описанные ниже.

А.42.5.1 Собрать стенд в соответствии со схемой (см. рисунок Рисунок 2).

А.42.5.2 Выполнить сравнение состава стенда с составом стенда, заявленным в RU.ВАТС.00180-01 92 02 «Специальное программное обеспечение подсистемы анализа информационно-технических объектов телекоммуникационных систем. Пусковой комплекс № 1. Стенд контроля железнодорожной АСУ ТП. Руководство пользователя».

А.42.5.3 Проверка в соответствии с пунктами А.42.5-А.42.5.2 считается выполненной успешно, если состав стенда соответствует составу стенда, заявленному в RU.ВАТС.00180-01 92 02 «Специальное программное обеспечение подсистемы анализа информационно-технических объектов телекоммуникационных систем. Пусковой комплекс № 1. Стенд контроля железнодорожной АСУ ТП. Руководство пользователя». В состав стенда входят типовые для моделируемых сфер датчики, исполнительные устройства.

А.42.5.4 На АРМ оператора АСУ ТП запустить программу ProgS_PLC в соответствии с RU.ВАТС.00180-01 92 02 «Специальное программное обеспечение подсистемы анализа информационно-технических объектов телекоммуникационных систем. Пусковой комплекс № 1. Стенд контроля железнодорожной АСУ ТП. Руководство пользователя».

А.42.5.5 В соответствии с RU.ВАТС.00180-01 92 02 «Специальное программное обеспечение подсистемы анализа информационно-технических объектов телекоммуникационных систем. Пусковой комплекс №1. Стенд контроля железнодорожной АСУ ТП. Руководство пользователя» в интерфейсе пользователя выполнить управление технологическими процессами:

- изменить скорость движения поездов на различных участках железной дороги;
- проверить индикацию состояния объектов инфраструктуры;
- опустить шлагбаумов при приближении поездов;
- проверить работу освещения в домах и на улице;
- проверить индикацию работы ТЭЦ.

А.42.5.6 Проверка в соответствии с пунктами А.42.5.4-А.42.5.5 считается выполненной успешно, если выполняется моделирование типовых технологических процессов.

А.42.6 Для проверки состава и работы пускового комплекса № 2 необходимо выполнить действия, описанные ниже.

А.42.6.1 Собрать стенд в соответствии со схемой (см. рисунок Рисунок 2).

А.42.6.2 Выполнить сравнение состава стенда с составом стенда, заявленным в RU.ВАТС.00180-01 92 03 «Специальное программное обеспечение подсистемы анализа информационно-технических объектов

телекоммуникационных систем. Пусковой комплекс № 2. Стенд контроля АСУ ТП систем жизнеобеспечения населенного пункта и производства. Руководство пользователя».

А.42.6.3 Проверка в соответствии с пунктами А.42.6-А.42.6.2 считается выполненной успешно, если в состав стенда соответствует составу стенда, заявленному в RU.BATC.00180-01 92 03 «Специальное программное обеспечение подсистемы анализа информационно-технических объектов телекоммуникационных систем. Пусковой комплекс № 2. Стенд контроля АСУ ТП систем жизнеобеспечения населенного пункта и производства. Руководство пользователя». В состав стенда входят типовые для моделируемых сфер датчики, исполнительные устройства.

А.42.6.4 На АРМ оператора АСУ ТП запустить программу ProgS_PLC в соответствии с RU.BATC.00180-01 92 03 «Специальное программное обеспечение подсистемы анализа информационно-технических объектов телекоммуникационных систем. Пусковой комплекс № 2. Стенд контроля АСУ ТП систем жизнеобеспечения населенного пункта и производства. Руководство пользователя».

А.42.6.5 В соответствии с RU.BATC.00180-01 92 03 «Специальное программное обеспечение подсистемы анализа информационно-технических объектов телекоммуникационных систем. Пусковой комплекс № 2. Стенд контроля АСУ ТП систем жизнеобеспечения населенного пункта и производства. Руководство пользователя» в интерфейсе пользователя выполнить управление технологическими процессами:

- выполнить имитацию протекания нефтепродуктов по нефтепроводу, путем перекачивания жидкости темного цвета;
- проверить индикацию уровня жидкостей в баках;
- проверить индикацию работы насосного агрегата путем вращения лопастей;
- проверить индикацию состояния (вкл./выкл.).

А.42.6.6 Проверка в соответствии с пунктами А.42.6.4-А.42.6.5 считается выполненной успешно, если выполняется моделирование типовых технологических процессов.

А.42.7 Для проверки пускового комплекса № 1 на обеспечение моделирования атак типа ARP-spoofing, приводящих к нарушениям моделируемых технологических процессов, необходимо выполнить действия, описанные ниже.

А.42.7.1 Собрать стенд в соответствии со схемой (см. рисунок Рисунок 2).

А.42.7.2 На АРМ злоумышленника из папки Scripts-S в консоли запустить набор скриптов в соответствии с RU.BATC.00180-01 92 02 «Специальное программное обеспечение подсистемы анализа информационно-технических объектов телекоммуникационных систем. Пусковой комплекс № 1. Стенд контроля железнодорожной АСУ ТП. Руководство пользователя».

А.42.7.3 В соответствии с RU.BATC.00180-01 92 02 «Специальное программное обеспечение подсистемы анализа информационно-технических объектов телекоммуникационных систем. Пусковой комплекс № 1. Стенд контроля железнодорожной АСУ ТП. Руководство пользователя» смоделировать атаки типа ARP-spoofing, приводящие к нарушениям моделируемых технологических процессов:

- типовое вредоносное информационное воздействие на сетевую инфраструктуру стенда;
- комплексное вредоносное информационное воздействие, направленное на изменение параметров технологического процесса на стенде с использованием специального программного обеспечения.

А.42.7.4 Проверка в соответствии с пунктами А.42.7-А.42.7.3 считается выполненной успешно, если в результате моделирования атак типа ARP-spoofing на пусковом комплексе № 1 произошло нарушение моделирования технологических процессов.

А.42.8 Для проверки пускового комплекса № 2 на обеспечение моделирования атак типа ARP-spoofing, приводящих к нарушениям моделируемых технологических процессов, необходимо выполнить действия, описанные ниже.

А.42.8.1 Собрать стенд в соответствии со схемой (см. рисунок Рисунок 2).

А.42.8.2 На АРМ злоумышленника из папки Scripts-E в консоли запустить набор скриптов в соответствии с RU.BATC.00180-01 92 03 «Специальное программное обеспечение подсистемы анализа информационно-технических объектов телекоммуникационных систем. Пусковой комплекс № 2. Стенд контроля АСУ ТП систем жизнеобеспечения населенного пункта и производства. Руководство пользователя».

А.42.8.3 В соответствии с RU.BATC.00180-01 92 03 «Специальное программное обеспечение подсистемы анализа информационно-технических объектов телекоммуникационных систем. Пусковой комплекс № 2. Стенд контроля АСУ ТП систем жизнеобеспечения населенного пункта и производства. Руководство пользователя» смоделировать атаки типа ARP-

spoofing, приводящие к нарушениям моделируемых технологических процессов:

- типовое вредоносное информационное воздействие на сетевую инфраструктуру стенда;
- комплексное вредоносное информационное воздействие, направленное на изменение параметров технологического процесса на стенде с использованием специального программного обеспечения.

А.42.8.4 Проверка в соответствии с пунктами А.42.8-А.42.8.3 считается выполненной успешно, если в результате моделирования атак типа ARP-spoofing, на пусковом комплексе № 2 произошло нарушение моделирования технологических процессов.

А.42.9 Для проверки реализации аварийных ситуаций на пусковом комплексе №1 необходимо выполнить действия, описанные ниже.

А.42.9.1 Собрать стенд в соответствии со схемой (см. рисунок Рисунок 2).

А.42.9.2 На АРМ злоумышленника запустить программу «Проверка реализации программы» в соответствии с RU.ВАТС.00180-01 92 02 «Специальное программное обеспечение подсистемы анализа информационно-технических объектов телекоммуникационных систем. Пусковой комплекс № 1. Стенд контроля железнодорожной АСУ ТП. Руководство пользователя».

А.42.9.3 В соответствии с RU.ВАТС.00180-01 92 02 «Специальное программное обеспечение подсистемы анализа информационно-технических объектов телекоммуникационных систем. Пусковой комплекс № 1. Стенд контроля железнодорожной АСУ ТП. Руководство пользователя» в интерфейсе пользователя выполнить моделирование аварийных ситуаций:

- несанкционированный перевод стрелок;
- столкновение составов;
- аварии при въезде в депо и на сортировочной горке;
- потеря контроля над скоростью движения поездов;
- выход из строя ТЭЦ и, как следствие, обесточивание всех объектов на стенде;
- сбои в работе шлагбаума.

А.42.9.4 Проверка в соответствии с пунктами А.42.9-А.42.9.3 считается выполненной успешно, если в результате их выполнения нарушение моделируемых технологических процессов сопровождается наглядными изменениями в работе макета (срабатывание световой сигнализации, столкновение объектов, выделение дыма и т.п.).

А.42.10 Для проверки реализации аварийных ситуаций на пусковом комплексе №2 необходимо выполнить действия, описанные ниже.

А.42.10.1 Собрать стенд в соответствии со схемой на рисунке Рисунок 2.

А.42.10.2 На АРМ злоумышленника запустить программу «Проверка реализации программы» в соответствии с RU.ВАТС.00180-01 92 03 «Специальное программное обеспечение подсистемы анализа информационно-технических объектов телекоммуникационных систем. Пусковой комплекс № 2. Стенд контроля АСУ ТП систем жизнеобеспечения населенного пункта и производства. Руководство пользователя».

А.42.10.3 В соответствии с RU.ВАТС.00180-01 92 03 «Специальное программное обеспечение подсистемы анализа информационно-технических объектов телекоммуникационных систем. Пусковой комплекс № 2. Стенд контроля АСУ ТП систем жизнеобеспечения населенного пункта и производства. Руководство пользователя» в интерфейсе пользователя выполнить моделирование аварийных ситуаций:

- несанкционированное перекрытие задвижек;
- несанкционированная остановка насосного агрегата;
- переполнение резервуаров;
- разливы сырья на поверхность макета;
- кавитация на насосном агрегате, сопровождаемая вибрацией насосного агрегата;
- перегрев насосного агрегата, сопровождаемый задымлением агрегата;
- задымление станции подогрева нефти в случае превышения рабочих температур.

А.42.10.4 Проверка в соответствии с пунктами А.42.10-А.42.10.3 считается выполненной успешно, если в результате их выполнения нарушение моделируемых технологических процессов сопровождается наглядными изменениями в работе макета (срабатывание световой сигнализации, столкновение объектов, выделение дыма и т.п.).

А.42.11 СПО ПОТ считается выдержавшим испытания по п. А.42.4-А.42.10.4 программы и методики испытаний и выполняющим пункты 3.2.4, 3.2.4.3 ТЗ на СЧ ОКР, если:

- создан стенд контроля информационно-технических объектов систем жизнеобеспечения с возможностью визуализации механизмов проведения воздействий в составе:
  - пусковой комплекс № 1 – стенд контроля железнодорожной АСУ ТП;

- пусковой комплекс № 2 – стенд контроля АСУ ТП систем жизнеобеспечения населенного пункта и производства;

- успешно завершены проверки пунктов А.42.4.4, А.42.4.9, А.42.5.3, А.42.5.6, А.42.6.3, А.42.6.6, А.42.7.4, А.42.8.4, А.42.9.4, А.42.10.4.

А.43 Методика № 43

А.43.1 В данной методике проводится проверка СПО ПОТ на соответствие требованиям пункта 3.2.4.4 ТЗ на СЧ ОКР «Амезит-В».

А.43.2 В соответствии с требованиями пунктов 3.2.4, 3.2.4.4 ТЗ на СЧ ОКР «Амезит-В» должен быть разработан сборник методик реверс-инжиниринга встроенного ПО (ВПО) в составе:

- методика восстановления схемотехнических особенностей ключевых узлов;
- методика определения наличия отладочных интерфейсов;
- методика получения образа управляющего ВПО за счет анализа ПО обновления (если присутствует) и считывания ПЗУ с помощью программатора;
- методика восстановления структуры хранения ВПО;
- методика определения базовой системы команд, расположения модулей ВПО в адресном пространстве микропроцессора;
- методика проведения исследований (реверса) модулей ВПО (статический анализ), определение ключевых алгоритмов взаимодействия компонентов и модулей;
- методика определения и восстановления алгоритмов, отвечающих за сетевое взаимодействие и обновление ВПО;
- методика анализа и описания возможностей технологических протоколов;
- методика анализа применяемых механизмов защиты ВПО от несанкционированного обновления
- методика модификации ВПО с целью проверки возможности внесения изменений;
- методика выделения ключевых компонентов (контроллеры, процессоры, память) на примере образца устройства Cisco;
- алгоритм установления взаимосвязи между ключевыми компонентами на примере образца устройства Cisco;
- алгоритм определения JTAG-интерфейса (на примере образца устройства Cisco;
- алгоритм определения UART-интерфейса (на примере образца устройства Cisco);

- анализ управляющих ключевых компонентов целевой системы на наличие внутренней памяти;
- алгоритм извлечения ВПО из внутренней памяти (при ее наличии) на примере образца устройства Cisco;
- описание особенностей получения образа управляющего ВПО из ПЗУ с помощью программатора;
- анализ ПО обновления на примере образца устройства Cisco;
- восстановление структуры хранения ВПО;
- разработка методики определения базовой си-стемы команд для характерных аппаратных платформ устройства Cisco;
- анализ расположения модулей ВПО в адресном пространстве микропроцессора и разработка алгоритма идентификации модулей ВПО на примере образца устройства Cisco.

А.43.3 Проверка выполняется согласно пунктам А.1.1-А.1.3.3 методики № Методика № 1.

А.43.4 СПО ПОТ считается выдержавшим испытания по п. А.43.3 программы и методики испытаний и выполняющим пункт 3.2.4.4 ТЗ на СЧ ОКР, если разработан сборник методик реверс-инжиниринга встроенного ПО (ВПО) в составе:

- методика восстановления схемотехнических особенностей ключевых узлов;
- методика определения наличия отладочных интерфейсов;
- методика получения образа управляющего ВПО за счет анализа ПО обновления (если присутствует) и считывания ПЗУ с помощью программатора;
- методика восстановления структуры хранения ВПО;
- методика определения базовой системы команд, расположения модулей ВПО в адресном пространстве микропроцессора;
- методика проведения исследований (реверса) модулей ВПО (статический анализ), определение ключевых алгоритмов взаимодействия компонентов и модулей;
- методика определения и восстановления алгоритмов, отвечающих за сетевое взаимодействие и обновление ВПО;
- методика анализа и описания возможностей технологических протоколов;
- методика анализа применяемых механизмов защиты ВПО от несанкционированного обновления
- методика модификации ВПО с целью проверки возможности внесения изменений;

- методика выделения ключевых компонентов (контроллеры, процессоры, память) на примере образца устройства Cisco;
- алгоритм установления взаимосвязи между ключевыми компонентами на примере образца устройства Cisco;
- алгоритм определения JTAG-интерфейса (на примере образца устройства Cisco;
- алгоритм определения UART-интерфейса (на примере образца устройства Cisco);
- анализ управляющих ключевых компонентов целевой системы на наличие внутренней памяти;
- алгоритм извлечения ВПО из внутренней памяти (при ее наличии) на примере образца устройства Cisco;
- описание особенностей получения образа управляющего ВПО из ПЗУ с помощью программатора;
- анализ ПО обновления на примере образца устройства Cisco;
- восстановление структуры хранения ВПО;
- разработка методики определения базовой системы команд для характерных аппаратных платформ устройства Cisco;
- анализ расположения модулей ВПО в адресном пространстве микропроцессора и разработка алгоритма идентификации модулей ВПО на примере образца устройства Cisco.

А.44 Методика № 44

А.44.1 В данной методике проводится проверка СПО ППА на соответствие требованиям пунктов 3.2.5, 3.2.5.1 на СЧ ОКР «Амезит-В».

А.44.2 В соответствии с требованиями пунктов 3.2.5, 3.2.5.1 ТЗ на СЧ ОКР «Амезит-В» СПО ППА должно обеспечивать анализ соединений технических средств автономного сегмента сети передачи данных и сбор информации.

А.44.3 Для проведения проверки СПО ППА на соответствие предъявляемым требованиям необходимо выполнить действия, описанные ниже.

А.44.3.1 Собрать испытательный стенд в соответствии со схемой (см. рисунок Рисунок 5).

А.44.3.2 Выполнить подключение генератора трафика (АПК СКАТ) к испытательному стенду. Порядок подключения генератора трафика (АПК СКАТ) и настройки испытательного стенда приведен в документе

RU.BATC.00181-01 32 01 «Специальное программное обеспечение подсистемы первичного анализа информации. Руководство системного программиста».

А.44.3.3 Выполнить запуск генератора трафика, который обеспечивает устойчивый трафик, проходящий через СПО съема трафика ППА с узла 10.10.10.15 по протоколу ftp. Порядок запуска и настройки генератора трафика приведен в документе RU.BATC.00181-01 32 01 «Специальное программное обеспечение подсистемы первичного анализа информации. Руководство системного программиста».

А.44.3.4 Выполнить вход в интерфейс оператора СПО съема трафика ППА и перейти в раздел настройки правил сбора трафика. Порядок действий приведен в документе RU.BATC.00181-01 34 01 «Специальное программное обеспечение подсистемы первичного анализа информации. Руководство оператора».

А.44.3.5 Выполнить ввод правил сбора трафика в интерфейсе оператора СПО съема трафика ППА (для IP-адреса 10.10.10.15 и протокола ftp). Порядок действий приведен в документе RU.BATC.00181-01 34 01 «Специальное программное обеспечение подсистемы первичного анализа информации. Руководство оператора».

А.44.3.6 Выполнить вход в интерфейс оператора СПО анализа трафика ППА и перейти в раздел просмотра статистики соединений. Порядок действий приведен в документе RU.BATC.00181-01 34 01 «Специальное программное обеспечение подсистемы первичного анализа информации. Руководство оператора».

А.44.3.7 Просмотреть статистику соединений и убедиться, что выполняется сбор трафика, соответствующего правилам, указанным в СПО съема трафика ППА, и анализ соединений технических средств автономного сегмента сети передачи данных. Порядок действий приведен в документе RU.BATC.00181-01 34 01 «Специальное программное обеспечение подсистемы первичного анализа информации. Руководство оператора».

А.44.4 СПО ППА считается выдержавшим испытания по п. А.44.3.1-А.44.3.7 программы и методики испытаний и выполняющим пункты 3.2.5, 3.2.5.1 ТЗ на СЧ ОКР, если пользователь при помощи СПО анализа трафика ППА может видеть соединения узла с IP адресом 10.10.10.15 по протоколу ftp.

А.45 Методика № 45

А.45.1 В данной методике проводится проверка СПО ППА на соответствие требованиям пунктов 3.2.5, 3.2.5.2 на СЧ ОКР «Амезит-В».

А.45.2 В соответствии с требованиями пунктов 3.2.5, 3.2.5.2 ТЗ на СЧ ОКР «Амезит-В» СПО ППА должно обеспечивать организацию узлов промежуточного контроля с целью получения доступа к информации, передаваемой с использованием протоколов типа IPSEC.

А.45.3 Для проведения проверки СПО ППА на соответствие предъявляемым требованиям необходимо выполнить действия, описанные ниже.

А.45.3.1 Собрать испытательный стенд в соответствии со схемой (см. рисунок Рисунок 5).

А.45.3.2 Выполнить подключение генератора трафика (АПК СКАТ) к испытательному стенду. Порядок подключения генератора трафика (АПК СКАТ) и настройки испытательного стенда приведен в документе RU.BATC.00181-01 32 01 «Специальное программное обеспечение подсистемы первичного анализа информации. Руководство системного программиста».

А.45.3.3 Выполнить запуск генератора трафика, который обеспечивает устойчивый трафик по протоколу IPSEC, проходящий через СПО съема трафика ППА (трафик моделирует вход на ресурс с парольно-адресной информацией: «user300» и «password300»). Порядок запуска и настройки генератора трафика приведен в документе RU.BATC.00181-01 32 01 «Специальное программное обеспечение подсистемы первичного анализа информации. Руководство системного программиста».

А.45.3.4 Выполнить подключение СПО съема трафика ППА (в качестве узла промежуточного контроля) к испытательному стенду. Порядок настройки испытательного стенда приведен в документе RU.BATC.00181-01 32 01 «Специальное программное обеспечение подсистемы первичного анализа информации. Руководство системного программиста».

А.45.3.5 Выполнить вход в интерфейс оператора СПО съема трафика ППА и указать необходимость сохранения трафика, использующего протокол IPSEC. Порядок действий приведен в документе RU.BATC.00181-01 34 01 «Специальное программное обеспечение подсистемы первичного анализа информации. Руководство оператора».

А.45.3.6 Выполнить вход в СПО съема трафика ППА, работающее на промежуточном узле, перейти в директорию, содержащую извлеченную парольно-адресную информацию. Инструкции по просмотру извлеченной парольно-адресной информации приведены в документе RU.BATC.00181-01 34 01 «Специальное программное обеспечение подсистемы первичного анализа информации. Руководство оператора».

А.45.3.7 Просмотреть файлы, содержащие парольно-адресную информацию. Убедиться, что организовано прохождение трафика через узел промежуточного контроля, которое обеспечивает получение доступа к информации, передаваемой с использованием протоколов типа IPSEC.

А.45.3.8 Выполнить вход в интерфейс оператора СПО съема трафика ППА и перейти в раздел просмотра сохраненного трафика. Порядок действий приведен в документе RU.ВАТС.00181-01 34 01 «Специальное программное обеспечение подсистемы первичного анализа информации. Руководство оператора».

А.45.3.9 Просмотреть содержимое файлов, содержащих сохраненный трафик. Убедиться, что трафик, содержащий протокол IPSEC, собран и сохранен для анализа в виде файлов формата «pcap». Порядок просмотра содержимого файлов приведен в документе RU.ВАТС.00181-01 34 01 «Специальное программное обеспечение подсистемы первичного анализа информации. Руководство пользователя».

А.45.4 СПО ППА считается выдержавшим испытания по п. А.45.3.1-А.45.3.9 программы и методики испытаний и выполняющим пункты 3.2.5, 3.2.5.2 ТЗ на СЧ ОКР, если оператор путем организации узла промежуточного контроля извлекает парольно-адресную информацию: «user300» и «password300».

А.46 Методика № 46

А.46.1 В данной методике проводится проверка СПО ППА на соответствие требованиям пунктов 3.2.5, 3.2.5.3 на СЧ ОКР «Амезит-В».

А.46.2 В соответствии с требованиями пунктов 3.2.5, 3.2.5.3 ТЗ на СЧ ОКР «Амезит-В» СПО ППА должно обеспечивать автоматическое распознавание и отбор файлов.

Примечания:

1. Перечень типов файлов, подлежащих распознаванию и отбору: HTML, GIF, JPEG, PNG, PDF, AVI, MPEG, DOC (DOCX), XLS (XLSX), PPT (PPTX), PPS, ZIP, GZIP, ARJ, RAR, BZIP, MP3, WAV, BMP, CDR, RTF, CSV, MPP, PST, XHTML, MHT, SXW, SXC, SXI, SXD, SXM, ODS, ODP, ODG, ODF, MDF, DBF, DB, MYD, DBQUERY, VSD.

2. Перечень протоколов, подлежащих распознаванию и анализу: FTP, HTTP, POP/POP3, IMAP, SMTP, SNMP, TELNET, Web-mail, SIP, H323, SKYPE, SSH, протоколы передачи электронных сообщений между пользователями (в том числе, протокол InstantMessaging), включая сообщения, отправляемые через сервисы социальных сетей.

3. Должны быть предусмотрены меры по предотвращению использования криптографически защищенных версий указанных протоколов.

А.46.3 Для проведения проверки СПО ППА на соответствие предъявляемым требованиям необходимо выполнить действия, описанные ниже.

А.46.3.1 Собрать испытательный стенд в соответствии со схемой (см. рисунок Рисунок 5).

А.46.3.2 Выполнить подключение генератора трафика (АПК СКАТ) к испытательному стенду. Порядок подключения генератора трафика (АПК СКАТ) и настройки испытательного стенда приведен в документе RU.ВАТС.00181-01 32 01 «Специальное программное обеспечение подсистемы первичного анализа информации. Руководство системного программиста».

А.46.3.3 Выполнить запуск генератора трафика, создающего трафик, в котором передаются файлы. Перечень передаваемых файлов приведен в приложении документа RU.ВАТС.00181-01 32 01 «Специальное программное обеспечение подсистемы первичного анализа информации. Руководство системного программиста».

А.46.3.4 Настроить передачу файлов. Порядок запуска и настройки генератора трафика приведен в документе RU.ВАТС.00181-01 32 01 «Специальное программное обеспечение подсистемы первичного анализа информации. Руководство системного программиста». В настройках указать протоколы:

- обращений к информационному ресурсу сети связи (протокол HTTP);
- передачи почтового e-mail-сообщения (протоколы smtp, pop3, imap, web-mail);
- передачи электронных сообщений между пользователями (протокол InstantMessaging), включая сообщения, отправляемые через сервисы социальных сетей, голосовой связи посредством сети передачи данных (протоколы SIP, H323, SKYPE);
- передачи файловых данных (протокол ftp);
- терминального доступа к оборудованию для удаленного управления (протоколы TELNET, SSH).

А.46.3.5 Выполнить вход в интерфейс оператора СПО съема трафика ППА и перейти в раздел настройки форматов распознаваемых файлов. Порядок действий приведен в документе RU.ВАТС.00181-01 34 01 «Специальное программное обеспечение подсистемы первичного анализа информации. Руководство оператора».

А.46.3.6 Выполнить ввод правил распознавания файлов. Перечень форматов распознаваемых файлов приведен в приложении документа RU.ВАТС.00181-01 32 01 «Специальное программное обеспечение подсистемы первичного анализа информации. Руководство системного программиста». Порядок действий по настройке правил распознавания приведен в документе RU.ВАТС.00181-01 34 01 «Специальное программное обеспечение подсистемы первичного анализа информации. Руководство оператора».

А.46.3.7 Выполнить ввод правил блокировки криптографически защищенных версий протоколов (FTP, HTTP, POP/POP3, IMAP, SMTP, SNMP, TELNET, Web-mail, SIP, H323, SKYPE, SSH, протоколы передачи электронных сообщений между пользователями (в том числе, протокол InstantMessaging), включая сообщения, отправляемые через сервисы социальных сетей). Порядок действий по настройке правил блокировки протоколов приведен в документе RU.ВАТС.00181-01 34 01 «Специальное программное обеспечение подсистемы первичного анализа информации. Руководство оператора».

А.46.3.8 Выполнить вход в интерфейс оператора СПО анализа трафика ППА и перейти в раздел просмотра результатов извлечения файлов из трафика. Порядок действий приведен в документе RU.ВАТС.00181-01 34 01 «Специальное программное обеспечение подсистемы первичного анализа информации. Руководство оператора».

А.46.3.9 Выполнить вход в интерфейс оператора СПО анализа трафика ППА и перейти в раздел просмотра результатов блокировки соединений. Порядок действий приведен в документе RU.ВАТС.00181-01 34 01 «Специальное программное обеспечение подсистемы первичного анализа информации. Руководство оператора».

А.46.3.10 Просмотреть результаты и убедиться, что в соответствии с настроенными правилами из трафика извлечены и сохранены файлы. Перечень файлов, их размеры и контрольные суммы соответствуют приведенным в приложении документа RU.ВАТС.00181-01 32 01 «Специальное программное обеспечение подсистемы первичного анализа информации. Руководство системного программиста».

А.46.3.11 Просмотреть результаты и убедиться, что в соответствии с настроенными правилами заблокированы соединения криптографически защищенных протоколов.

А.46.4 СПО ППА считается выдержавшим испытания по п. А.46.3.1-А.46.3.11 программы и методики испытаний и выполняющим пункты 3.2.5, 3.2.5.3 ТЗ на СЧ ОКР, если пользователь при помощи СПО может настраивать правила, обеспечивающие автоматическое распознавание и извлечение файлов

и в соответствии с перечнем протоколов (FTP, HTTP, POP/POP3, IMAP, SMTP, SNMP, TELNET, Web-mail, SIP, H323, SKYPE, SSH, протоколы передачи электронных сообщений между пользователями (в том числе, протокол InstantMessaging)).

А.47 Методика № 47

А.47.1 В данной методике проводится проверка СПО ППА на соответствие требованиям пунктов 3.2.5, 3.2.5.4 на СЧ ОКР «Амезит-В».

А.47.2 В соответствии с требованиями пунктов 3.2.5, 3.2.5.4 ТЗ на СЧ ОКР «Амезит-В» СПО ППА должно обеспечивать автоматизированную подготовку и развертывание в автономном сегменте сети передачи данных «двойников» для легитимных ресурсов ГИС ОП.

Примечание: в качестве технологии создания «двойников» для легитимных ресурсов использовать:

- для статических ресурсов – копирование информации до третей степени вложенности;
- для динамических ресурсов – копирование главной страницы с возможностью регистрации идентификационной информации (парольной адресной информацией).

А.47.3 Для проведения проверки СПО ППА на соответствие предъявляемым требованиям необходимо выполнить действия, описанные ниже.

А.47.3.1 Собрать испытательный стенд в соответствии со схемой (см. рисунок Рисунок 5).

А.47.3.2 Выполнить вход в интерфейс оператора СПО создания «двойников» легитимных ресурсов ГИС ОП и перейти в раздел создания «двойников» статических ресурсов. Порядок создания сайтов-«двойников» приведен в документе RU.ВАТС.00181-01 34 01 «Специальное программное обеспечение подсистемы первичного анализа информации. Руководство оператора».

А.47.3.3 Указать адрес исходного легитимного ресурса ГИС ОП (news1000.ru), для которого необходимо создать сайт-«двойник». Структура исходного ресурса должна состоять из статических веб-страниц.

А.47.3.4 Указать адрес, по которому должно быть выполнено развертывание сайта-«двойника».

А.47.3.5 Запустить процедуру создания сайта-«двойника».

А.47.3.6 По окончании процедуры копирования просмотреть структуру страниц сайта-«двойника», расположенного по адресу развертывания.

Убедиться, что выполнено копирование информации до третьей степени вложенности исходного легитимного ресурса.

А.47.3.7 Выполнить вход в интерфейс оператора СПО создания «двойников» легитимных ресурсов ГИС ОП, перейти в раздел создания «двойников» динамических ресурсов. Порядок действий приведен в документе RU.ВАТС.00181-01 34 01 «Специальное программное обеспечение подсистемы первичного анализа информации. Руководство оператора».

А.47.3.8 Указать адрес исходного легитимного ресурса ГИС ОП, для которого необходимо создать сайт-«двойник». Структура исходного ресурса должна состоять из динамических веб-страниц.

А.47.3.9 Указать адрес, по которому должно быть выполнено развертывание сайта-«двойника».

А.47.3.10 Запустить процедуру создания сайта-«двойника».

А.47.3.11 По окончании процедуры просмотреть структуру страниц сайта-«двойника», расположенного по адресу развертывания. Убедиться, что выполнено копирование главной страницы с возможностью регистрации идентификационной информации (парольной адресной информации) исходного ресурса. Порядок просмотра копии развернутого сайта-«двойника» приведен в документе RU.ВАТС.00181-01 34 01 «Специальное программное обеспечение подсистемы первичного анализа информации. Руководство оператора».

А.47.4 СПО ППА считается выдержавшим испытания по п. А.47.3.1-А.47.3.11 программы и методики испытаний и выполняющим пункты 3.2.5, 3.2.5.4 ТЗ на СЧ ОКР, если пользователь при помощи СПО создания «двойников» легитимных ресурсов ГИС ОП смог осуществить автоматизированную подготовку и развертывание в автономном сегменте сети передачи данных двайника для ресурса news1000.ru.

А.48 Методика № 48

А.48.1 В данной методике проводится проверка СПО ППА на соответствие требованиям пунктов 3.2.5, 3.2.5.5 на СЧ ОКР «Амезит-В».

А.48.2 В соответствии с требованиями пунктов 3.2.5, 3.2.5.5 ТЗ на СЧ ОКР «Амезит-В» СПО ППА должно обеспечивать блокировку и перенаправление клиентских запросов (HTTP/HTTPS) на легитимные ресурсы ГИС ОП (зеркала).

Примечания:

1. Блокируемые ресурсы задаются в виде списка URL (содержащего hostname или IP).
2. Должна быть возможность для блокируемого ресурса указать IP адрес веб-сервера, на который следует перенаправить поступающий запрос.

3. Должна быть предусмотрена возможность организаций нескольких зеркал (с различным наполнением) на одном IP-адресе.

А.48.3 Для проведения проверки СПО ППА на соответствие предъявляемым требованиям необходимо выполнить действия, описанные ниже.

А.48.3.1 Собрать испытательный стенд в соответствии со схемой (см. рисунок Рисунок 5).

А.48.3.2 Выполнить вход в интерфейс оператора СПО съема трафика ППА и перейти в раздел настройки «двойников» ресурсов ГИС ОП. Порядок действий приведен в документе RU.BATC.00181-01 34 01 «Специальное программное обеспечение подсистемы первичного анализа информации. Руководство оператора».

А.48.3.3 В интерфейсе оператора СПО съема трафика ППА задать перечень URL (news1000.ru), которые определяют список ресурсов, запросы к которым (по протоколам HTTP, HTTPS) должны быть перенаправлены. Порядок настройки списка перенаправляемых ресурсов приведен в документе RU.BATC.00181-01 34 01 «Специальное программное обеспечение подсистемы первичного анализа информации. Руководство оператора».

А.48.3.4 В интерфейсе оператора СПО съема трафика ППА задать перечень URL (news2000.ru и news3000.ru), определяющих подготовленные сайты-«двойники» ГИС ОП. Порядок действий приведен в документе RU.BATC.00181-01 34 01 «Специальное программное обеспечение подсистемы первичного анализа информации. Руководство оператора».

А.48.3.5 Запустить обозреватель на АРМ оператора, подключенном к автономному сегменту, и выполнить клиентский запрос к ресурсу (news1000.ru), который должен быть перенаправлен на подготовленный сайт-«двойник».

А.48.3.6 Просмотреть веб-страницу, отображаемую обозревателем, и убедиться, что было выполнено перенаправление запроса на сайт-«двойник» (news2000.ru).

А.48.4 СПО ППА считается выдержавшим испытания по п. А.48.3.1-А.48.3.6 программы и методики испытаний и выполняющим пункты 3.2.5, 3.2.5.5 ТЗ на СЧ ОКР, если:

- СПО ППА обеспечивает перенаправление клиентских (HTTP, HTTPS) запросов к news1000.ru на подготовленные сайты-«двойники» ГИС ОП (news2000.ru и news3000.ru);

- оператор СПО съема трафика ППА имеет возможность настройки перечня ресурсов, запрос к которым должен быть перенаправлен (news1000.ru);

- оператор СПО съема трафика ППА имеет возможность настройки перечня сайтов-«двойников», на которые следует перенаправлять запрос(news2000.ru и news3000.ru);.

А.49 Методика № 49

А.49.1 В данной методике проводится проверка СПО ППА на соответствие требованиям пунктов 3.2.5, 3.2.5.6 на СЧ ОКР «Амезит-В».

А.49.2 В соответствии с требованиями пунктов 3.2.5, 3.2.5.6 ТЗ на СЧ ОКР «Амезит-В» СПО ППА должно обеспечивать возможность выбора заданного абонента автономного сегмента сети передачи данных путем задания оператором совокупности коммутационно-адресных признаков, в том числе IP-адреса, IP-маски, MAC-адреса, адреса для протоколов прикладного уровня.

А.49.3 Для проведения проверки СПО ППА на соответствие предъявляемым требованиям необходимо выполнить действия, описанные ниже.

А.49.3.1 Собрать испытательный стенд в соответствии со схемой (см. рисунок Рисунок 5).

А.49.3.2 Выполнить вход в интерфейс оператора СПО съема трафика ПКС и перейти в раздел ввода правил сохранения трафика абонента. Порядок действий по вводу правил сохранения трафика абонента приведен в документе RU.BATC.00181-01 34 01 «Специальное программное обеспечение подсистемы первичного анализа информации. Руководство оператора».

А.49.3.3 Просмотреть форму ввода и убедиться, что оператор имеет возможность выбора заданного абонента путем задания совокупности коммутационно-адресных признаков, в том числе IP-адреса (10.10.10.15), IP-маски (255.255.255.0), MAC-адреса, адреса протоколов прикладного уровня (ftp).

А.49.4 СПО ППА считается выдержавшим испытания по п. А.49.3.1-А.49.3.3 программы и методики испытаний и выполняющим пункты 3.2.5, 3.2.5.6 ТЗ на СЧ ОКР, если оператор в интерфейсе СПО съема трафика ППА при вводе правил отбора и сохранения трафика абонента имеет возможность выбора абонента путем задания (10.10.10.15), IP-маски (255.255.255.0), MAC-адреса, адреса протоколов прикладного уровня (ftp).

А.50 Методика № 50

А.50.1 В данной методике проводится проверка СПО ППА на соответствие требованиям пунктов 3.2.5, 3.2.5.7 на СЧ ОКР «Амезит-В».

А.50.2 В соответствии с требованиями пунктов 3.2.5, 3.2.5.7 ТЗ на СЧ ОКР «Амезит-В» СПО ППА должно обеспечивать выявление каналов передачи данных систем связи и управления противодействующей стороны.

А.50.3 Для проведения проверки СПО ППА на соответствие предъявляемым требованиям необходимо выполнить действия, описанные ниже.

А.50.3.1 Собрать испытательный стенд в соответствии со схемой (см. рисунок Рисунок 5).

А.50.3.2 Выполнить подключение генератора трафика (АПК СКАТ) к испытательному стенду. Порядок подключения генератора трафика (АПК СКАТ) и настройки испытательного стенда приведен в документе RU.ВАТС.00181-01 32 01 «Специальное программное обеспечение подсистемы первичного анализа информации. Руководство системного программиста».

А.50.3.3 Выполнить вход в интерфейс оператора СПО съема трафика ППА и перейти в раздел настройки правил выявления каналов передачи данных систем связи и управления противодействующей стороны. Порядок действий приведен в документе RU.ВАТС.00181-01 34 01 «Специальное программное обеспечение подсистемы первичного анализа информации. Руководство оператора».

А.50.3.4 Ввести правила выявления каналов передачи данных систем связи и управления противодействующей стороны, задавая критерии «подозрительности» (соединения с IP адресом 10.10.10.100 и протоколом ftp). Порядок задания критериев приведен в документе RU.ВАТС.00181-01 34 01 «Специальное программное обеспечение подсистемы первичного анализа информации. Руководство оператора».

А.50.3.5 Запустить генератор трафика для создания трафика, моделирующего каналы передачи данных систем связи и управления противодействующей стороны, проходящего через СПО съема трафика ППА. Порядок запуска и настройки генератора трафика приведен в документе RU.ВАТС.00181-01 32 01 «Специальное программное обеспечение подсистемы первичного анализа информации. Руководство системного программиста».

А.50.3.6 Выполнить вход в интерфейс оператора СПО анализа трафика ППА и перейти в раздел просмотра сообщений о выявленных каналах передачи данных систем связи и управления противодействующей стороны.

А.50.3.7 Просмотреть сообщения о выявлении каналов передачи данных и убедиться, что из проходящего трафика выявлены каналы передачи данных систем связи и управления противоборствующей стороны, а по каждому выявленному каналу отображается следующая информация:

- время соединения;
- абонент (IP-адрес, порт);
- получатель (IP-адрес, порт);
- протокол;
- объем трафика.

А.50.4 СПО ППА считается выдержавшим испытания по п. А.50.3.1-А.50.3.7 программы и методики испытаний и выполняющим пункты 3.2.5, 3.2.5.7 ТЗ на СЧ ОКР, если:

- СПО ППА обеспечивает выявление каналов передачи данных систем связи и управления противодействующей стороны путем выявления соединений, соответствующих критериям «подозрительности» (соединения с IP адресом 10.10.10.100 и протоколом ftp);
- пользователь в интерфейсе оператора СПО анализа трафика ППА может видеть сообщения о выявлении каналов передачи данных систем связи и управления противодействующей стороны, содержащие информацию: время соединения, абонент (IP-адрес, порт), получатель (IP-адрес, порт), протокол, объем трафика: 14:56:10; 10.10.10.100:21; 192.168.1.10:1329; ftp; 105300 байт.

А.51 Методика № 51

А.51.1 В данной методике проводится проверка СПО ППА на соответствие требованиям пунктов 3.2.5, 3.2.5.8 на СЧ ОКР «Амезит-В».

А.51.2 В соответствии с требованиями пунктов 3.2.5, 3.2.5.8 ТЗ на СЧ ОКР «Амезит-В» СПО ППА должно обеспечивать нарушение штатного функционирования коммуникационного оборудования с использованием технических средств контроля объектов телекоммуникационных систем.

А.51.3 Для проведения проверки СПО ППА на соответствие предъявляемым требованиям необходимо выполнить действия, описанные ниже.

А.51.3.1 Собрать испытательный стенд в соответствии со схемой (см. рисунок Рисунок 5).

А.51.3.2 Выполнить вход в интерфейс оператора СПО съема трафика ППА и перейти в раздел настойки трафика, предназначенного для нарушения штатного функционирования коммуникационного оборудования противодействующей стороны. Порядок действий приведен в документе RU.BATC.00181-01 34 01 «Специальное программное обеспечение подсистемы первичного анализа информации. Руководство оператора».

А.51.3.3 Указав IP-адрес 10.10.10.200, выбрать в интерфейсе оператора СПО съема трафика ППА коммуникационное оборудование (техническое

средство контроля объектов телекоммуникационных систем), работа которого должна быть нарушена. Порядок действий приведен в документе RU.BATC.00181-01 34 01 «Специальное программное обеспечение подсистемы первичного анализа информации. Руководство оператора».

A.51.3.4 В интерфейсе оператора СПО съема трафика ППА выбрать файл (attack_pcap), содержащий сохраненный трафик со специально подготовленными параметрами пакетов и предназначенный для нарушения штатного функционирования коммуникационного оборудования. Порядок действий приведен в документе RU.BATC.00181-01 34 01 «Специальное программное обеспечение подсистемы первичного анализа информации. Руководство оператора».

A.51.3.5 В интерфейсе оператора СПО съема трафика ППА запустить цикличную передачу сохраненного трафика на коммуникационное оборудование. Порядок действий приведен в документе RU.BATC.00181-01 34 01 «Специальное программное обеспечение подсистемы первичного анализа информации. Руководство оператора».

A.51.3.6 Выполнить вход в консоль управления технического средства 10.10.10.200 (коммутатора Extreme Summit X670-48). Убедиться, что вход в консоль управления затруднен (или невозможен) по причине нарушения штатного функционирования коммуникационного оборудования. Порядок входа в консоль управления технического средства приведен в документе RU.BATC.00181-01 32 01 «Специальное программное обеспечение подсистемы первичного анализа информации. Руководство системного программиста».

A.51.4 СПО ППА считается выдержавшим испытания по п. A.51.3.1-A.51.3.6 программы и методики испытаний и выполняющим пункты 3.2.5, 3.2.5.8 ТЗ на СЧ ОКР, если СПО ППА обеспечивает передачу на узел по IP-адресу 10.10.10.200 сохраненного трафика со специально подготовленными параметрами (файл attack_pcap).

A.52 Методика № 52

A.52.1 В данной методике проводится проверка СПО ППА на соответствие требованиям пунктов 3.2.5, 3.2.5.9 на СЧ ОКР «Амезит-В».

A.52.2 В соответствии с требованиями пунктов 3.2.5, 3.2.5.9 ТЗ на СЧ ОКР «Амезит-В» СПО ППА должно обеспечивать определение режима работы и состава телекоммуникационного оборудования.

A.52.3 Для проведения проверки СПО ППА на соответствие предъявляемым требованиям необходимо выполнить действия, описанные ниже.

А.52.3.1 Собрать испытательный стенд в соответствии со схемой (см. рисунок Рисунок 5).

А.52.3.2 Выполнить вход в интерфейс оператора СПО съема трафика ППА и перейти в раздел просмотра режима работы и состава телекоммуникационного оборудования. Порядок действий приведен в документе RU.BATC.00181-01 34 01 «Специальное программное обеспечение подсистемы первичного анализа информации. Руководство оператора».

А.52.3.3 Запустить подготовку отчета, содержащего режимы работы и состав телекоммуникационного оборудования узла по адресу 10.10.10.200. Порядок формирования отчета приведен в документе RU.BATC.00181-01 34 01 «Специальное программное обеспечение подсистемы первичного анализа информации. Руководство оператора».

А.52.3.4 Просмотреть сформированный отчет и убедиться, что для оборудования определен и отображен режим работы, а также приведен состав телекоммуникационного оборудования.

А.52.3.5 Просмотреть содержимое сформированного отчета и убедиться, что при отображении режима работы и состава телекоммуникационного оборудования показана следующая информация:

- статус оборудования (работает/не работает);
- использованные протоколы;
- тип оборудования.

А.52.4 СПО ППА считается выдержавшим испытания по п. А.52.3.1-А.52.3.5 программы и методики испытаний и выполняющим пункты 3.2.5, 3.2.5.9 ТЗ на СЧ ОКР, если СПО ППА обеспечивает определение режима работы и состава узла телекоммуникационного оборудования 10.10.10.200.

А.53 Методика № 53

А.53.1 В данной методике проводится проверка СПО ППА на соответствие требованиям пунктов 3.2.5, 3.2.5.10 на СЧ ОКР «Амезит-В».

А.53.2 В соответствии с требованиями пунктов 3.2.5, 3.2.5.10 ТЗ на СЧ ОКР «Амезит-В» СПО ППА должно обеспечивать выявление каналов передачи данных критически важных информационных объектов.

А.53.3 Для проведения проверки СПО ППА на соответствие предъявляемым требованиям необходимо выполнить действия, описанные ниже.

А.53.3.1 Собрать испытательный стенд в соответствии со схемой (см. рисунок Рисунок 5).

А.53.3.2 Выполнить подключение генератора трафика (АПК СКАТ) к испытательному стенду. Порядок подключения генератора трафика (АПК СКАТ) и настройки испытательного стенда приведен в документе RU.ВАТС.00181-01 32 01 «Специальное программное обеспечение подсистемы первичного анализа информации. Руководство системного программиста».

А.53.3.3 Выполнить вход в интерфейс оператора СПО съема трафика ППА и перейти в раздел настройки правил выявления каналов передачи данных критически важных информационных объектов. Порядок настройки правил приведен в документе RU.ВАТС.00181-01 34 01 «Специальное программное обеспечение подсистемы первичного анализа информации. Руководство оператора».

А.53.3.4 Ввести правила выявления каналов передачи данных критически важных информационных объектов, задавая набор критериев (соединения с IP адресом 10.10.10.11 и протоколом SNMP).

А.53.3.5 Запустить генератор трафика для создания трафика, содержащего каналы передачи данных критически важных информационных объектов и проходящего через СПО съема трафика ППА (file_SNMP). Порядок запуска и настройки генератора трафика приведен в документе RU.ВАТС.00181-01 32 01 «Специальное программное обеспечение подсистемы первичного анализа информации. Руководство системного программиста».

А.53.3.6 Выполнить вход в интерфейс оператора СПО анализа трафика ППА и перейти в раздел просмотра сообщений о выявленных каналах передачи данных критически важных информационных объектов. Порядок просмотра сообщений приведен в документе RU.ВАТС.00181-01 34 01 «Специальное программное обеспечение подсистемы первичного анализа информации. Руководство оператора».

А.53.3.7 Просмотреть сообщения о выявлении каналов передачи данных и убедиться, что из проходящего трафика выявлены каналы передачи данных критически важных информационных объектов, а по каждому выявленному каналу отображается следующая информация:

- время соединения;
- абонент (IP-адрес, порт);
- получатель (IP-адрес, порт);
- протокол;
- объем трафика.

А.53.4 СПО ППА считается выдержавшим испытания по п. А.53.3.1-А.53.3.7 программы и методики испытаний и выполняющим пункты 3.2.5, 3.2.5.10 ТЗ на СЧ ОКР, если:

- СПО ППА обеспечивает выявление каналов передачи данных критически важных информационных объектов соединения с IP адресом 10.10.10.11 и протоколом SNMP.

А.54 Методика № 54

А.54.1 В данной методике проводится проверка СПО ППА на соответствие требованиям пунктов 3.2.5, 3.2.5.11 на СЧ ОКР «Амезит-В».

А.54.2 В соответствии с требованиями пунктов 3.2.5, 3.2.5.11 ТЗ на СЧ ОКР «Амезит-В» СПО ППА должно обеспечивать выявление информационных ресурсов противодействующей стороны.

А.54.3 Для проведения проверки СПО ППА на соответствие предъявляемым требованиям необходимо выполнить действия, описанные ниже.

А.54.3.1 Собрать испытательный стенд в соответствии со схемой (см. рисунок Рисунок 5).

А.54.3.2 Выполнить подключение генератора трафика (АПК СКАТ) к испытательному стенду. Порядок подключения генератора трафика (АПК СКАТ) и настройки испытательного стенда приведен в документе RU.BATC.00181-01 32 01 «Специальное программное обеспечение подсистемы первичного анализа информации. Руководство системного программиста».

А.54.3.3 Выполнить вход в интерфейс оператора СПО съема трафика ППА и перейти в раздел настройки правил выявления информационных ресурсов противодействующей стороны. Порядок настройки правил выявления информационных ресурсов приведен в документе RU.BATC.00181-01 34 01 «Специальное программное обеспечение подсистемы первичного анализа информации. Руководство оператора».

А.54.3.4 Ввести правила выявления информационных ресурсов противодействующей стороны, задавая набор критериев соединения к IP адресу 10.10.10.115 по порту 13333.

А.54.3.5 Запустить генератор трафика для создания трафика, содержащего соединения к IP адресу 10.10.10.115 по порту 13333 (файл pcap_13333) и проходящего через СПО съема трафика ППА. Ресурсы задаются набором критериев: IP-адрес, порт, протокол, URL, имя хоста (SNI), Common Name (CN). Порядок запуска и настройки генератора трафика приведен в документе RU.BATC.00181-01 32 01 «Специальное программное обеспечение подсистемы первичного анализа информации. Руководство системного программиста».

А.54.3.6 Выполнить вход в интерфейс оператора СПО анализа трафика ППА и перейти в раздел просмотра сообщений о выявленных ресурсах противодействующей стороны. Порядок просмотра сообщений приведен в документе RU.ВАТС.00181-01 34 01 «Специальное программное обеспечение подсистемы первичного анализа информации. Руководство оператора».

А.54.3.7 Просмотреть сообщения о выявлении ресурсов и убедиться, что из проходящего трафика выявлены информационные ресурсы противодействующей стороны, характеристики которых соответствуют заранее заданным критериям.

А.54.4 СПО ППА считается выдержавшим испытания по п. А.54.3.1-А.54.3.7 программы и методики испытаний и выполняющим пункты 3.2.5, 3.2.5.11 ТЗ на СЧ ОКР, если:

- пользователь в интерфейсе оператора СПО анализа трафика ППА может видеть сообщения о выявлении ресурсов противодействующей стороны, содержащие следующую информацию: соединения к узлу с IP адресом 10.10.10.115 по порту 13333.

А.55 Методика № 55

А.55.1 В данной методике проводится проверка СПО ППА на соответствие требованиям пунктов 3.2.5, 3.2.5.12 на СЧ ОКР «Амезит-В».

А.55.2 В соответствии с требованиями пунктов 3.2.5, 3.2.5.12 ТЗ на СЧ ОКР «Амезит-В» СПО ППА должно обеспечивать регистрацию в накопитель информационного обмена (в полном объеме) абонента, задаваемого оператором.

А.55.3 Для проведения проверки СПО ППА на соответствие предъявляемым требованиям необходимо выполнить действия, описанные ниже.

А.55.3.1 Собрать испытательный стенд в соответствии со схемой (см. рисунок Рисунок 5).

А.55.3.2 Выполнить подключение генератора трафика (АПК СКАТ) к испытательному стенду. Порядок подключения генератора трафика (АПК СКАТ) и настройки испытательного стенда приведен в документе RU.ВАТС.00181-01 32 01 «Специальное программное обеспечение подсистемы первичного анализа информации. Руководство системного программиста».

А.55.3.3 Выполнить вход в интерфейс оператора СПО съема трафика ППА и перейти в раздел настройки правил, определяющих абонента, трафик которого следует сохранить. Порядок действий приведен в документе

RU.BATC.00181-01 34 01 «Специальное программное обеспечение подсистемы первичного анализа информации. Руководство оператора».

А.55.3.4 Ввести правила сохранения трафика в интерфейсе оператора СПО съема трафика ППА для выбранного абонента соединения к IP адресу 10.10.10.111 по протоколу ftp. Порядок ввода правил приведен в документе RU.BATC.00181-01 34 01 «Специальное программное обеспечение подсистемы первичного анализа информации. Руководство оператора».

А.55.3.5 Запустить генератор трафика для создания устойчивого информационного обмена от имени выбранного абонента, проходящего через СПО съема трафика ППА (передается файл testdataftp). Порядок запуска и настройки генератора трафика приведен в документе RU.BATC.00181-01 32 01 «Специальное программное обеспечение подсистемы первичного анализа информации. Руководство системного программиста».

А.55.3.6 Выполнить вход в интерфейс оператора СПО анализа трафика ППА и перейти в раздел просмотра сохраненного трафика. Порядок действий по просмотру сохраненного трафика приведен в документе RU.BATC.00181-01 34 01 «Специальное программное обеспечение подсистемы первичного анализа информации. Руководство оператора».

А.55.3.7 Просмотреть содержимое файлов, содержащих сохраненный трафик, и убедиться, что трафик абонента, заданного оператором, сохранен в виде файлов формата «pcap». Порядок просмотра содержимого файлов приведен в документе RU.BATC.00181-01 34 01 «Специальное программное обеспечение подсистемы первичного анализа информации. Руководство оператора».

А.55.3.8 Выполнить вход в интерфейс оператора СПО анализа трафика ППА и перейти в раздел просмотра статистики соединений. Порядок действий приведен в документе RU.BATC.00181-01 34 01 «Специальное программное обеспечение подсистемы первичного анализа информации. Руководство оператора».

А.55.3.9 Просмотреть статистку соединений абонента, выбранного оператором, и сравнить размеры файлов, содержащих сохраненный трафик, с объемом переданного трафика из статистики соединений. Убедиться, что информационный обмен абонента, заданного оператором, зарегистрирован в накопитель информационного обмена (в полном объеме).

А.55.4 СПО ППА считается выдержавшим испытания по п. А.55.3.1-А.55.3.9 программы и методики испытаний и выполняющим пункты 3.2.5, 3.2.5.12 ТЗ на СЧ ОКР, если:

- пользователь при помощи СПО съема трафика ППА смог выполнить настройку правил съема трафика по IP-адресу 10.10.10.111 по протоколу ftp;
- СПО съема трафика ППА выполнило съем и сохранение файла test-dataftp для соединения к IP-адресу 10.10.10.111 по протоколу ftp.

А.56 Методика № 56

А.56.1 В данной методике проводится проверка СПО ППА на соответствие требованиям пунктов 3.2.5, 3.2.5.13 на СЧ ОКР «Амезит-В».

А.56.2 В соответствии с требованиями пунктов 3.2.5, 3.2.5.13 ТЗ на СЧ ОКР «Амезит-В» программные средства первичного анализа информации должны обеспечивать выполнение требований назначения на скоростях до 10 Гбит/с при выполнении условия «нормальности» трафика, а также на скоростях до 6 Гбит/с для трафика, не удовлетворяющего условию «нормальности».

А.56.3 Для проведения проверки СПО ППА на соответствие предъявляемым требованиям необходимо выполнить действия, описанные ниже.

А.56.3.1 Собрать испытательный стенд в соответствии со схемой (см. рисунок Рисунок 5).

А.56.3.2 Выполнить подключение генератора трафика (АПК СКАТ) к испытательному стенду. Порядок подключения генератора трафика (АПК СКАТ) и настройки испытательного стенда приведен в документе RU.ВАТС.00181-01 32 01 «Специальное программное обеспечение подсистемы первичного анализа информации. Руководство системного программиста».

А.56.3.3 Выполнить вход в интерфейс настройки генератора трафика, установить параметры генерации трафика со скоростью 10 Гбит/с (доля коротких пакетов (длиной до 64 байт) не превышает 20 %). Порядок запуска и настройки генератора трафика приведен в документе RU.ВАТС.00181-01 32 01 «Специальное программное обеспечение подсистемы первичного анализа информации. Руководство системного программиста».

А.56.3.4 Выполнить вход в интерфейс оператора СПО анализа трафика ППА и перейти в раздел просмотра статистики. Порядок действий приведен в документе RU.ВАТС.00181-01 34 01 «Специальное программное обеспечение подсистемы первичного анализа информации. Руководство оператора».

А.56.3.5 Просмотреть статистику трафика и убедиться, что скорость трафика, поступающего в СПО анализа трафика ППА, соответствует требованиям пункта 3.2.5.13 ТЗ.

А.56.3.6 Выполнить вход в интерфейс настройки генератора трафика, установить параметры непрерывной генерации трафика со скоростью 6 Гбит/с (доля коротких пакетов (длиной до 64 байт) превышает 20 %). Порядок действий по настройке приведен в документе RU.BATC.00181-01 32 01 «Специальное программное обеспечение подсистемы первичного анализа информации. Руководство системного программиста».

А.56.3.7 Выполнить вход в интерфейс оператора СПО анализа трафика ППА и перейти в раздел просмотра статистики. Порядок действий приведен в документе RU.BATC.00181-01 34 01 «Специальное программное обеспечение подсистемы первичного анализа информации. Руководство оператора».

А.56.3.8 Просмотреть статистику трафика и убедиться, что скорость трафика, поступающего в СПО анализа трафика ППА, соответствует требованиям пункта 3.2.5.13 ТЗ на СЧ ОКР.

А.56.4 СПО ППА считается выдержавшим испытания по п. А.56.3.1-А.56.3.8 программы и методики испытаний и выполняющим пункты 3.2.5, 3.2.5.13 ТЗ на СЧ ОКР, если отчет показывает, что программные средства первичного анализа информации обеспечивают обработку трафика на скоростях до 10 Гбит/с при выполнении условия «нормальности» трафика, а также на скоростях до 6 Гбит/с для трафика, неудовлетворяющего условию «нормальности».

А.57 Методика № 57

А.57.1 В данной методике проводится проверка СПО ППА на соответствие требованиям пунктов 3.2.5, 3.2.5.14 на СЧ ОКР «Амезит-В».

А.57.2 В соответствии с требованиями пунктов 3.2.5, 3.2.5.14 ТЗ на СЧ ОКР «Амезит-В» СПО ППА должно обеспечивать сопряжение с каналообразующей аппаратурой различных опорных сетей передачи данных.

Примечание. Перечень стыков уточняется по результатам эскизного и технического (при необходимости) проектирования и согласовывается с головным исполнителем.

А.57.3 Для проведения проверки СПО ППА на соответствие предъявляемым требованиям необходимо выполнить действия, описанные ниже.

А.57.3.1 Собрать испытательный стенд в соответствии со схемой (см. рисунок Рисунок 5).

А.57.3.2 Используя комплект патч-кордов (содержащий коннекторы типов FC, SC, ST, LC), выполнить подключение маршрутизатора D-link DGS-1100-24 испытательного стенда к каналообразующей аппаратуре опорных сетей

передачи данных (каналу связи со стендом, моделирующим сегмент сети Интернет). Порядок настройки испытательного стенда приведен в документе RU.BATC.00181-01 32 01 «Специальное программное обеспечение подсистемы первичного анализа информации. Руководство системного программиста».

А.57.3.3 Используя интерфейсы типа Ethernet и SFP, выполнить подключение серверов ППА к испытательному стенду. Порядок настройки испытательного стенда приведен в документе RU.BATC.00181-01 32 01 «Специальное программное обеспечение подсистемы первичного анализа информации. Руководство системного программиста».

А.57.3.4 Запустить обозреватель на АРМ оператора, подключенном к испытательному стенду, и выполнить запрос на доступ к информационному ресурсу сети Интернет (к сайту yandex.ru).

А.57.3.5 Выполнить вход в интерфейс оператора СПО ППА. Просмотреть статистику соединений и убедиться, что испытательный стенд подключен к каналообразующей аппаратуре опорных сетей передачи данных (существует запись об успешном соединении АРМ оператора с yandex.ru). Порядок действий по просмотру статистики приведен в документе RU.BATC.00181-01 34 01 «Специальное программное обеспечение подсистемы первичного анализа информации. Руководство оператора».

А.57.4 СПО ППА считается выдержавшим испытания по п. А.57.3.1-А.57.3.5 программы и методики испытаний и выполняющим пункты 3.2.5, 3.2.5.14 ТЗ на СЧ ОКР, если пользователь с АРМ оператора смог загрузить страницу yandex.ru.

А.58 Методика № 58

А.58.1 В данной методике проводится проверка СПО ПРД на соответствие требованиям пунктов 3.2.6, 3.2.6.1 ТЗ на СЧ ОКР «Амезит-В».

А.58.2 В соответствии с требованиями пунктов 3.2.6, 3.2.6.1 ТЗ на СЧ ОКР «Амезит-В» СПО ПРД должно обеспечивать выполнение функций ретрансляции данных в целях реализации скрытого обмена между техническими средствами мониторинга сети Интернет и ресурсами ГИС Интернет по протоколам семейства TCP/IP.

А.58.3 Для проведения проверки СПО ПРД на соответствие предъявляемым требованиям необходимо выполнить действия, описанные ниже.

А.58.3.1 Запустить обозреватель и перейти на страницу авторизации интерфейса управления СПО ПРД.

А.58.3.2 Произвести авторизацию в интерфейсе управления с использованием учетных данных системного программиста (администратора).

А.58.3.3 Перейти в раздел «Маршруты».

А.58.3.4 Создать маршрут типа Tor с названием «Маршрут Tor», в качестве правила выбора выходного узла – выбрать правило типа «По стране» и задать двухбуквенный код произвольной Европейской страны (например, FR для Франция или DE для Германии).

А.58.3.5 Перейти в раздел «Правила» и создать правило типа «подсеть» для подсистемы СПО ПМС с названиями «ПМС».

А.58.3.6 Назначить созданному ~~пользователю~~ правилу маршрут «Маршрут Tor».

А.58.3.7 Для созданного ~~пользователя~~ правила отключить проверку прикладных настроек.

А.58.3.8 На АРМ пользователя ПМС запустить обозреватель и открыть адрес: http://2ip.ru.

А.58.3.9 Проверить соответствие страны, определенной сервисом, и страны выходного узла, заданной в маршруте «Маршрут Tor».

А.58.3.10 Перейти на адрес сервиса: https://check.torproject.orghttps://whoer.net/.

А.58.3.11 Убедиться, что выводится сообщение «This browser is configured to use Tor.»

А.58.4 СПО ПРД считается выдержавшим испытания по п. А.58.3.1-А.58.3.11 программы и методики испытаний и выполняющим пункты 3.2.6, 3.2.6.1 ТЗ на СЧ ОКР, если:

- при выполнении вышеуказанных действий данной методики отсутствовали сообщения об ошибках;
- при выполнении пп. А.58.3.2 была произведена успешная авторизация в интерфейс управления;
- при выполнении пп. А.58.3.4 в таблице маршрутов появился созданный маршрут;
- при выполнении пп. А.58.3.5 в таблице правил появлось созданное правило;
- страна, определенная сервисом, соответствует заданной стране;
- сервис check.torproject.org подтверждает использование анонимизации Tor сообщением «This browser is configured to use Tor.».

А.59 Методика № 59

А.59.1 В данной методике проводится проверка СПО ПРД на соответствие требованиям пунктов 3.2.6, 3.2.6.2 ТЗ на СЧ ОКР «Амезит-В».

А.59.2 В соответствии с требованиями пунктов 3.2.6, 3.2.6.2 ТЗ на СЧ ОКР «Амезит-В» СПО ПРД должно обеспечивать выполнение функций ретрансляции данных в целях реализации скрытого обмена между техническими средствами подготовки, размещения и «раскрутки» специальных материалов и ресурсами ГИС Интернет по протоколам семейства TCP/IP.

Примечания:

1. Критериями скрытности обмена являются возможности по противодействию подсистемы ПРД следующим признакам обмена информацией с использованием виртуальных маршрутов:

- однотипность исходящего трафика;
- долгосрочное использование узлов подсистемы ПРД;
- однотипность узлов (в том числе, управляющих).

2. К критериям скрытности обмена также относятся:

- возможности подсистемы ПРД противостоять атакам на трафик;
- защищенность клиентской части подсистемы ПРД от атак, направленным на прикладное ПО с целью получения реального сетевого адреса;
- защищенность узлов серверной части от атак, направленных на получение несанкционированного доступа.

3. В качестве протоколов ретрансляции данных использовать Tor и VPN-туннели.

А.59.3 Для проведения проверки СПО ПРД на соответствие предъявляемым требованиям необходимо выполнить действия, описанные ниже.

А.59.3.1 Запустить обозреватель и перейти на страницу авторизации интерфейса управления СПО ПРД.

А.59.3.2 Произвести авторизацию в интерфейсе управления с использованием учетных данных системного программиста (администратора).

А.59.3.3 Перейти в раздел «Маршруты».

А.59.3.4 Создать маршрут типа VPN с названием «Маршрут VPN».

А.59.3.5 В правиле выбора выходного узла в поле IP-адрес выбрать произвольный доступный IP-адрес.

А.59.3.6 Задать значение «Время жизни» – 180.

А.59.3.7 Сохранить созданный маршрут.

А.59.3.8 Перейти в раздел «Правила» и создать правило типа «подсеть» для подсистемы СПО ПРР с названием «ПРР».

А.59.3.9 В созданном правиле ввести IP-адрес АРМ ПРР и выбрать маску подсети «255.255.255.0».

А.59.3.10 Назначить созданному правилу маршрут «Маршрут VPN».

А.59.3.11 Отключить проверку прикладных настроек в данном правиле.

А.59.3.12 На АРМ пользователя ПРР запустить обозреватель и открыть адрес: http://internet.yandex.ru.

А.59.3.13 Проверить соответствие отображаемого IPv4-адреса правилу выходного узла в маршруте «Маршрут VPN».

А.59.3.14 На АРМ пользователя ПРД перейти в раздел «Туннели».

А.59.3.15 Выбрать туннель «Маршрут VPN» и записать список используемых узлов в туннеле.

А.59.3.16 Дождаться перестроения туннеля «Маршрут VPN».

А.59.3.17 Проверить, что длительность использования узлов подсистемы ПРД определяется временнем жизни туннеля, для этого сверить список используемых узлов в карточке нового туннеля с узлами, использованными ранее.

А.59.3.18 Проверить наличие в списке туннелей записей «Маршрут VPN» и «Маршрут Tor».

А.59.3.19 Перейти в раздел «Правила».

А.59.3.20 Выбрать правило «ПРР».

А.59.3.21 В значении параметра «Прикладные настройки» указать «Индивидуальный».

А.59.3.22 Выбрать значение «запретить» для следующих параметров: Webrtc, AdobeFlash, ActiveX, Java.

А.59.3.23 На АРМ пользователя ПМС открыть адрес: https://browserleaks.com/webrtc

А.59.3.24 Проверить, что пользовательское ПО защищенно от атаки на получение реальных локальных и публичных IP-адресов – в полях Local IP Address и Public IP Address не должно отображаться пользовательских IP-адресов.

А.59.3.25 На АРМ пользователя ПРД перейти в раздел «Узлы» и выписать IP-адреса (<IP-1> и <IP-2>) двух произвольных узлов.

А.59.3.26 Запустить программу для каждого из адресов со следующими флагами:

nmap –sT –n <IP-1>

nmap –sT –n <IP-2>

А.59.3.27 Проверить неоднотипность узлов – выводимые при сканировании порты сервисов различаются.

А.59.4 СПО ПРД считается выдержавшим испытания по п. А.59.3.1-А.59.3.27 программы и методики испытаний и выполняющим пункты 3.2.6, 3.2.6.2 ТЗ на СЧ ОКР, если:

- при выполнении вышеуказанных действий данной методики отсутствовали сообщения об ошибках;
- в таблице маршрутов появился созданный маршрут «Маршрут VPN»;
- в таблице правил отобразилось созданное правило;
- отображаемый в сервисе http://internet.yandex.ru IPv4-адрес соответствует IPv4-адресу заданного выходного узла VPN маршрута.
- успешно проведена проверка методики Методика № 58, в ходе которой подтверждается поддержка ретрансляции с использованием Tor по маршруту «Маршрут Tor»;
- успешно проведена проверка использования различных узлов при перестроении туннелей ретрансляции;
- успешно проведена проверка защищенности от получения реального IP-адреса пользователя (внутреннего и внешнего);
- успешно проведена проверка различия сетевого сканирования узлов ретрансляции;
- успешно проведена проверка методики Методика № 77, включающая проверку возможности подсистемы ПРД противостоять атакам на трафик и защищенность узлов серверной части от атак, направленных на получение несанкционированного доступа.

А.60 Методика № 60

А.60.1 В данной методике проводится проверка СПО ПРД на соответствие требованиям пунктов 3.2.6, 3.2.6.3 ТЗ на СЧ ОКР «Амезит-В».

А.60.2 В соответствии с требованиями пунктов 3.2.6, 3.2.6.3 ТЗ на СЧ ОКР «Амезит-В» СПО ПРД должно обеспечивать построение рациональных, с точки зрения скрытности и скорости обмена информацией виртуальных транспортных маршрутов ретрансляции данных.

Примечания:

1. При построении маршрутов должны использоваться шаблоны построения виртуальных транспортных маршрутов, созданные администратором.
2. Должно быть разработано средство подготовки шаблонов, также выполняющее задачу оценки работоспособности, скрытности и скорости обмена информацией.

А.60.3 Для проведения проверки СПО ПРД на соответствие предъявляемым требованиям необходимо выполнить действия, описанные ниже.

А.60.3.1 Запустить обозреватель и перейти на страницу авторизации интерфейса управления СПО ПРД.

А.60.3.2 Произвести авторизацию в интерфейсе управления с использованием учетных данных системного программиста (администратора).

А.60.3.3 Перейти в раздел «Маршруты».

А.60.3.4 Выбрать произвольный активный VPN-маршрут.

А.60.3.5 Открыть панель «Туннели».

А.60.3.6 Проверить, что туннели ретрансляции строятся в соответствии с правилами в маршруте – выходной узел текущего туннеля должен правилу выбора выходного узла маршрута (для VPN-маршрута свойства узла находятся во всплывающей подсказке к полю с IP-адресом).

А.60.3.7 Инициировать создание нового шаблона маршрута нажатием кнопки «Создать».

А.60.3.8 Выбрать тип маршрута «VPN».

А.60.3.9 Задать длину маршрута «3».

А.60.3.10 Активировать панель «Правила».

А.60.3.11 Проверить для всех правил возможность выбора типов критериев: Группа, Страна, IP-адрес.

А.60.3.12 Проверить, что при изменении в произвольном правиле любого критерия:

- изменяется количество доступных узлов в карточке данного правила в строке: «Узлов: <количество узлов>»;
- изменяется количество возможных маршрутов в строке «Возможные маршруты: <количество возможных маршрутов>».

А.60.3.13 Увеличить длину маршрута на одно правило.

А.60.3.14 Проверить работу функции прогнозирования скорости – должны изменяться значения в строках «Мин. скорость» и «Макс. скорость» в карточке маршрута.

А.60.3.15 Задать в каждом правиле цепочки по одному IP-адресу узла.

А.60.3.16 Проверить работу функции оценки скрытности – в карточке маршрута в строке «Скрытность» должно отобразиться значение «Минимальная».

А.60.3.17 Удалить во всех правилах критерии.

А.60.3.18 Проверить работу функции оценки скрытности – карточке маршрута отображается в строке «Скрытность» значение «Высокая» (при условии, что количество доступных узлов в каждой карточке не менее 3).

А.60.4 СПО ПРД считается выдержавшим испытания по п. А.60.3.1-А.60.3.18 программы и методики испытаний и выполняющим пункты 3.2.6, 3.2.6.3 ТЗ на СЧ ОКР, если:

- при выполнении вышеуказанных действий данной методики отсутствовали сообщения об ошибках;
- была произведена успешная авторизация в интерфейс управления;
- построенние туннелей маршрутов происходит в соответствии с заданными правилами в маршруте (проверка выходного адреса туннеля маршрута выполнена успешно);
- в средстве редактирования маршрутов доступна возможность задания следующих типов критериев выбора узлов: Группа, Страна, IP-адрес;
- успешно проведена проверка работы функции прогнозирования скрытности и скорости обмена информацией при редактировании правил маршрута.

А.61 Методика № 61

А.61.1 В данной методике проводится проверка СПО ПРД на соответствие требованиям пунктов 3.2.6, 3.2.6.4 ТЗ на СЧ ОКР «Амезит-В».

А.61.2 В соответствии с требованиями пунктов 3.2.6, 3.2.6.4 ТЗ на СЧ ОКР «Амезит-В» СПО ПРД должно обеспечивать подключение автоматизированных рабочих мест операторов АПК «Амезит» к системе обмена данными, не требующее дополнительных настроек для пользователей.

А.61.3 Для проведения проверки СПО ПРД на соответствие предъявляемым требованиям необходимо выполнить действия, описанные ниже.

А.61.3.1 На АРМ пользователя ПРД открыть «Центр управления сетями и общим доступом».

А.61.3.2 Перейти в раздел «Изменение параметров адаптеров».

А.61.3.3 Нажать правой кнопкой мыши на сетевом интерфейсе Ethernet (Подключение по локальной сети).

А.61.3.4 В контекстном меню выбрать пункт «Свойства».

А.61.3.5 Выбрать в списке «Протокол Интернета версии 4 (TCP/IPv4)» и нажать на кнопку «Свойства».

А.61.3.6 На вкладке «Общие» выбрать «Получить IP-адрес автоматически» и «Получить адрес DNS-сервера автоматически».

А.61.3.7 Подключить АРМ пользователя ПРД к коммутатору ПРД.

А.61.3.8 На АРМ пользователя запустить обозреватель и проверить наличие доступа к ресурсам ГИС Интернет, открыв произвольный интернет-ресурс.

А.61.3.9 Проверить маскирование географического расположения пользователя, воспользовавшись общедоступными сервисами по идентификации местонахождения интернет-пользователей: https://geoiptool.com.

А.61.3.10 Проверить, что отображаемое географическое расположение пользователя отличается от физического.

А.61.4 СПО ПРД считается выдержавшим испытания по п. А.61.3.1-А.61.3.10 программы и методики испытаний и выполняющим пункты 3.2.6, 3.2.6.4 ТЗ на СЧ ОКР, если:

- при выполнении вышеуказанных действий данной методики отсутствовали сообщения об ошибках;
- была успешно открыта страница произвольного интернет-ресурса;
- проверка географического расположения не оторазила реального географического положения пользователя.

А.62 Методика № 62

А.62.1 В данной методике проводится проверка СПО ПРД на соответствие требованиям пунктов 3.2.6, 3.2.6.5 ТЗ на СЧ ОКР «Амезит-В».

А.62.2 В соответствии с требованиями пунктов 3.2.6, 3.2.6.5 ТЗ на СЧ ОКР «Амезит-В» СПО ПРД должно обеспечивать автоматическое построение виртуальных маршрутов с заданной глубиной через заданные интервалы времени. Должны быть предусмотрены механизмы конфигурирования и контроля построения виртуальных маршрутов.

А.62.3 Для проведения проверки СПО ПРД на соответствие предъявляемым требованиям необходимо выполнить действия, описанные ниже.

А.62.3.1 Запустить обозреватель и перейти на страницу авторизации интерфейса управления СПО ПРД.

А.62.3.2 Произвести авторизацию в интерфейсе управления с использованием учетных данных системного программиста (администратора).

А.62.3.3 Перейти в раздел «Маршруты».

А.62.3.4 Инициировать создание нового маршрута нажатием кнопки «Создать».

А.62.3.5 Выбрать тип маршрута «VPN».

А.62.3.6 В карточке нового маршрута убедиться в наличии параметров: Тип, Длина маршрута, Время жизни маршрута.

А.62.3.7 Выбрать любой имеющийся активный маршрут типа VPN.

А.62.3.8 Открыть панель «Туннели».

А.62.3.9 Убедиться, что периодичность построения новых туннелей соответствует параметру времени жизни, заданного для маршрута (колонки – «время создания» и «время завершения»), с погрешностью не более двух минут.

А.62.3.10 Перейти в раздел «Туннели».

А.62.3.11 Нажать правой кнопкой мыши на любой активный туннель типа VPN.

А.62.3.12 Проверить наличие кнопок «Перестроить» и «Закрыть» в карточке туннеля.

А.62.3.13 Нажать кнопку «Перестроить».

А.62.3.14 Вернуться в раздел «Маршруты» и выбрать маршрут для туннеля, для которого было инициировано перестроение.

А.62.3.15 Открыть панель «Туннели».

А.62.3.16 Убедиться в изменении активного туннеля по данному маршруту (время перестроения туннеля может занимать до 5 минут).

А.62.4 СПО ПРД считается выдержавшим испытания по п. А.62.3.1-А.62.3.16 программы и методики испытаний и выполняющим пункты 3.2.6, 3.2.6.5 ТЗ на СЧ ОКР, если:

- при выполнении вышеуказанных действий данной методики отсутствовали сообщения об ошибках;
- произведена успешная авторизация в интерфейс управления;
- в маршруте доступны параметры: Тип, Длина маршрута, Время жизни;
- разница между временем создания и временем завершения туннеля соответствовует времени жизни маршрута;
- администратору доступны кнопки «Перестроить» и «Закрыть» для активных туннелей;
- запросу администратора был успешно перестроен туннель по маршруту(при перестроении туннеля происходит закрытие текущего и создание нового).

А.63 Методика № 63

А.63.1 В данной методике проводится проверка СПО ПРД на соответствие требованиям пунктов 3.2.6, 3.2.6.6 ТЗ на СЧ ОКР «Амезит-В».

А.63.2 В соответствии с требованиями пунктов 3.2.6, 3.2.6.6 ТЗ на СЧ ОКР «Амезит-В» СПО ПРД должно обеспечивать сокрытие персонализирующей информации о средствах передачи данных от средств мониторинга и анализа противодействующей стороны;

Примечание. К персонализирующим атрибутам средств передачи данных относятся:

- сетевые адреса (MAC-, IP-адреса), принадлежащие (или идентифицируемые как аппаратные средства) МО РФ;
- особенности сетевого взаимодействия, свойственные сертифицированным в РФ операционным системам;
- прикладное программное обеспечение (в том числе, СЗИ), используемое в РФ.

А.63.3 Для проведения проверки СПО ПРД на соответствие предъявляемым требованиям необходимо выполнить действия, описанные ниже.

А.63.3.1 Запустить обозреватель и перейти на страницу авторизации интерфейса управления СПО ПРД.

А.63.3.2 Произвести авторизацию в интерфейсе управления с использованием учетных данных системного программиста (администратора).

А.63.3.3 Перейти в раздел «Правила».

А.63.3.4 Выбрать правило «ПМС».

А.63.3.5 Убедиться, что правило настроено для доступа к ресурсам ГИС Интернет через маршрут «Маршрут Tor».

А.63.3.6 Открыть список прокси маршрутов, перейдя в подраздел «Прокси маршрутов» раздела «Настройки».

А.63.3.7 Записать IP-адрес и порт прокси-сервиса для маршрута «Маршрут Tor».

А.63.3.8 Перейти в раздел «Узлы».

А.63.3.9 Выбрать любой узел, на котором доступен https-сервер. Наличие https-сервера можно проверить в панели «Активные сервисы» карточки туннеля. В случае отсутствия таких узлов необходимо обратиться к документу RU.ВАТС.00182-01 32 01 «Специальное программное обеспечение подсистемы ретрансляции данных с использованием промежуточных серверов. Руководство системного программиста» для генерации и установки на узле ретрансляции пакета ПО, включающего https веб-сервер.

А.63.3.10 Получить IP-адрес и данные для доступа по SSH для узла с работающим https веб-сервером.

А.63.3.11 Подключиться к узлу ретрансляции по SSH (согласно документу RU.BATC.00182-01 32 01 «Специальное программное обеспечение подсистемы ретрансляции данных с использованием промежуточных серверов. Руководство системного программиста») с АРМ пользователя ПРД, используя данные пункта А.63.3.10.

А.63.3.12 В терминале SSH-сессии запустить следующую команду:

```
tcpdump -i <сетевой интерфейс с IP-адресом узла> tcp port 443 <порт VPN-сервера>
-w /tmp/traffic.pcap
```

А.63.3.13 Выполнить следующие действия на АРМ пользователя согласно документу RU.BATC.00177-01 92 04 «Специальное программное обеспечение подсистемы формирования автономного сегмента сети передачи данных. Программное обеспечение «Wireshark». Руководство пользователя»:

А.63.3.14 Запустить Wireshark.

А.63.3.15 Выбрать интерфейс подключения к локальной сети для анализа трафика.

А.63.3.16 Запустить анализ трафика.

А.63.3.17 Запустить обозреватель.

А.63.3.18 В обозревателе открыть адрес: https://<IP-адрес-узла-ретрансляции>:<порт VPN-сервера>/

А.63.3.19 В обозревателе открыть адрес: http://myexternalip.com/raw

А.63.3.20 Записать отображенный IP-адрес.

А.63.3.21 Закрыть обозреватель.

А.63.3.22 Остановить анализ трафика в Wireshark.

А.63.3.23 Сохранить файл трафика в файл с именем: pc_traffic.pcap.

А.63.3.24 На АРМ пользователя ПРД в окне SSH-соединения прервать запись данных с сетевого интерфейса, нажав комбинацию клавиш «Ctrl+C».

А.63.3.25 Переместить файл /tmp/traffic.pcap в директорию https веб-сервера (обратиться к документу RU.BATC.00182-01 32 01 «Специальное программное обеспечение подсистемы ретрансляции данных с использованием промежуточных серверов. Руководство системного программиста» для определения данной директории), выполнив команды:

```
chmod a+r /tmp/traffic.pcap
mv /tmp/traffic.pcap <path-to-web-dir (/var/www/fhs по-умолчанию)>
```

А.63.3.26 Используя АРМ пользователя ПМС, запустить обозреватель и скачать файл данных с узла ретрансляции, перейдя по ссылке: https://<IP-адрес-узла-ретрансляции>>:<порт VPN-сервера>/traffic.pcap.

А.63.3.27 Скопировать полученные файлы traffic.pcap и pc_traffic.pcap на АРМ пользователя ПРД, используя USB-флеш-накопитель.

А.63.3.28 Запустить Wireshark и открыть файл traffic.pcap. Отфильтровать трафик, используя выражение фильтра: ip.addr == <–IP~~ip~~-адрес пункта http://myexternalip.com/raw> and tcp.port == ~~443~~<порт VPN-сервера>.

А.63.3.29 Запустить Wireshark и открыть файл pc_traffic.pcap. Отфильтровать трафик, используя выражение фильтра: ip.addr == <–IP-адрес узла ретрансляции~~адрес для доступа по SSH~~> ~~and~~ or socks.remote_name == <IP-адрес узла ретрансляции> or tcp.port == <порт прокси-сервиса маршута «Маршрут Tor»~~tcp.port == 443~~.

А.63.3.30 Проверить, что персонализирующие признаки в пакетах АРМ пользователя ПМС не попадают на узлы ретрансляции:

- IP-адрес источника в исходящих пакетах pc_traffic.pcap не должен быть обнаружен в пакетах traffic.pcap;
- MAC-адрес источника в исходящих пакетах pc_traffic.pcap не должен быть обнаружен в пакетах traffic.pcap.

А.63.3.31 На АРМ ПРР открыть ссылку в обозревателе: https://bit.ly/2Jb7jzR

А.63.3.32 Подключиться с помощью SSH-клиента к серверу управления и выполнить команду: sudo netstat –ntp | grep 37.9.96.20

А.63.3.33 Проверить, что соединение к серверу 37.9.96.20 от клиента ПРД терминируются на сервере управления и взаимодействие с целевым сервисом выполняется от имени прикладного посредника на сервере управления, что исключает утечку особенностей сетевого взаимодействия клиентских операционных систем, а также любого другого программного обеспечению на сетевом уровне. Для этого вывод команды должен содержать строки следующего формата:

```
tcp 0 0 <IP адрес на сервере управления>:<порт> 37.9.96.20:443 ESTABLISHED
<pid>/socks
```

А.63.3.34 Дождаться открытия ссылки или прервать загрузку по ссылке на АРМ ПРР.

А.63.3.35 В ssh-сессии повторно выполнить команду:

```
sudo netstat -ntp | grep 37.9.96.20
```

А.63.3.36 Проверить, что установленное ранее соединение с целевым сервисом закрывается прикладным посредником после завершения получения данных на АРМ пользователя ПРР. Вывод команды должен быть пустым или содержать строку, сообщающую о закрытом соединении:

```
tcp 0 0 <IP адрес на сервере управления>:<порт> 37.9.96.20:443 TIME_WAIT <pid>/
socks
```

А.63.4 СПО ПРД считается выдержавшим испытания по п. А.63.3.1-А.63.3.36 программы и методики испытаний и выполняющим пункты 3.2.6, 3.2.6.6 ТЗ на СЧ ОКР, если:

- при выполнении вышеуказанных действий данной методики отсутствовали сообщения об ошибках;
- была произведена успешная авторизация в интерфейс управления;
- были были успешно получены IP-адрес и данные для доступа по SSH для узла;
- при сравнении файлов трафика не было выявлено совпадающих персонализирующих признаков;
- успешно проведена проверка блокировки утечек особенностей сетевого взаимодейтсвия, свойственные сертифицированным в РФ операционным системам и прикладному программному обеспечению.

А.64 Методика № 64

А.64.1 В данной методике проводится проверка СПО ПРД на соответствие требованиям пунктов 3.2.6, 3.2.6.7 ТЗ на СЧ ОКР «Амезит-В».

А.64.2 В соответствии с требованиями пунктов 3.2.6, 3.2.6.7 ТЗ на СЧ ОКР «Амезит-В» СПО ПРД должно обеспечивать сокрытие информации о национальной принадлежности.

А.64.3 Для проведения проверки СПО ПРД на соответствие предъявляемым требованиям необходимо выполнить действия, описанные ниже.

А.64.3.1 Выполнить пункты А.61.3.1-А.61.3.7 методики № Методика № 61.

А.64.3.2 Запустить командую строку на АРМ пользователя, выполнив следующие действия:

- нажать комбинацию клавиш «Win+R»;
- в открывшемся окне запуска ввести: cmd.exe;
- нажать на клавишу «Enter».

А.64.3.3 В командной строке выполнить команду: ipconfig.

А.64.3.4 Результат выполнения команды будет содержать IP-адрес АРМ пользователя.

А.64.3.5 Согласно документу RU.BATC.00182-01 34 01 «Специальное программное обеспечение подсистемы ретрансляции данных с использованием промежуточных серверов. Руководство оператора» установить и запустить СПО КПН.

А.64.3.6 Согласно документу RU.BATC.00182-01 92 01 «Специальное программное обеспечение подсистемы ретрансляции данных с использованием промежуточных серверов. Руководство пользователя» выполнить действия, описанные ниже.

А.64.3.7 Запустить обозреватель и перейти на страницу авторизации интерфейса управления СПО ПРД.

А.64.3.8 Произвести авторизацию в интерфейсе управления с использованием учетных данных системного программиста (администратора).

А.64.3.9 Перейти в раздел «Правила» и создать новое правило с названием «АРМ ПРД».

А.64.3.10 Ввести для правила IP-адрес, полученный при выполнении пункта А.64.3.4, и маску 255.255.255.255.

А.64.3.11 Выбрать в поле маршрут: «Маршрут Tor» (созданный при выполнении методики № Методика № 58).

А.64.3.12 В поле «Прикладные настройки» выбрать значение «Индивидуальный».

А.64.3.13 Для всех параметров прикладных настроек установить значение «Разрешить».

А.64.3.14 Установить значение параметра «Часовой пояс» любое значение, отличное от временной зоны города Москвы.

А.64.3.15 Выбрать только одну раскладку в параметре «Языковые раскладки» – «en_US Английский (Соединенные Штаты)».

А.64.3.16 Сохранить созданное правило.

А.64.3.17 На АРМ оператора, согласно документу RU.BATC.00182-01 34 01 «Специальное программное обеспечение подсистемы ретрансляции данных с использованием промежуточных серверов. Руководство оператора», скорректировать настройки системы для предоставления доступа к ресурсам ГИС Интернет.

А.64.3.18 Запустить обозреватель и проверить наличие доступа к ресурсам ГИС Интернет, открыв произвольный интернет-ресурс.

А.64.3.19 Проверить маскирование национальной принадлежности, воспользовавшись общедоступным сервиом по проверке отпечатка интернет-обозревателя (https://geoiptool.com). При проверке определенное местоположение пользователя не должно совпадать с реальным.

А.64.4 СПО ПРД считается выдержавшим испытания по п. А.64.3.1-А.64.3.19 программы и методики испытаний и выполняющим пункты 3.2.6, 3.2.6.7 ТЗ на СЧ ОКР, если:

- при выполнении вышеуказанных действий данной методики отсутствовали сообщения об ошибках;
- результат выполнения команды ipconfig содержал IP-адрес АРМ пользователя;
- была произведена успешная авторизация в интерфейс управления;
- в таблице правил появилось созданное правило;
- было успешно выполнено маскирование национальной принадлежности.

А.65 Методика № 65

А.65.1 В данной методике проводится проверка СПО ПРД на соответствие требованиям пунктов 3.2.6, 3.2.6.8 ТЗ на СЧ ОКР «Амезит-В».

А.65.2 В соответствии с требованиями пунктов 3.2.6, 3.2.6.8 ТЗ на СЧ ОКР «Амезит-В» СПО ПРД должно обеспечивать маскирование данных на узлах ретрансляции под легальные пользовательские запросы к общедоступным сервисам следующими способами:

- размещение публичных прокси-серверов на узлах ретрансляции данных;
- размещение выходных узлов TOR на узлах ретрансляции данных;
- размещение I2P-роутеров на узлах ретрансляции данных.

Способ маскирования данных на узлах ретрансляции определяется администратором.

Для каждого из способов должна обеспечиваться возможность создания дистрибутива с необходимым ПО и настройками, пригодного для установки администратором на заданный узел ретрансляции данных.

Примечание. При создании дистрибутива необходимо обеспечить различие настроек ПО с целью недопущения вскрытия узлов подсистемы ПРД на основании этого признака или разработать средство дополнительной настройки.

А.65.3 Для проведения проверки СПО ПРД на соответствие предъявляемым требованиям необходимо выполнить действия, описанные ниже.

А.65.3.1 Запустить обозреватель и перейти на страницу авторизации интерфейса управления СПО ПРД.

А.65.3.2 Произвести авторизацию в интерфейсе управления с использованием учетных данных системного программиста (администратора).

А.65.3.3 Перейти в раздел «Узлы».

А.65.3.4 Выбрать любой доступный узел группы «Выходной».

А.65.3.5 Записать его IP-адрес и номер узла.

А.65.3.6 Открыть панель «Данные о доступе».

А.65.3.7 Записать данные для доступа по SSH.

А.65.3.8 Перейти в раздел «Маршруты».

А.65.3.9 Выбрать маршрут «Маршрут VPN».

А.65.3.10 Очистить критерии выбора выходного узла (последнее правило выбора узлов).

А.65.3.11 В качестве критерия выбора выходного узла указать IP-адрес, полученный в пункте А.65.3.5.

А.65.3.12 Сохранить маршрут.

А.65.3.13 Подключиться к серверу управления СПО ПРД по SSH от имени суперпользователя (согласно документу RU.ВАТС.00182-01 32 01 «Специальное программное обеспечение подсистемы ретрансляции данных с использованием промежуточных серверов. Руководство системного программиста»).

А.65.3.14 Согласно документу RU.ВАТС.00182-01 32 01 «Специальное программное обеспечение подсистемы ретрансляции данных с использованием промежуточных серверов. Руководство системного программиста» сгенерировать дистрибутив для узла, выбранного в пункте А.65.3.11 в качестве выходного. Дистрибутив должен включать:

- tor – в режиме exit-node;
- i2p-роутер;
- прокси-сервер;
- маскирование OpenVPN через https-сервер.

А.65.3.15 Установить полученный дистрибутив на выходной узел ретрансляции «Маршрута VPN».

А.65.3.16 Перейти в раздел «Правила».

А.65.3.17 Отключить доступ в Интернет всем правилам, работающим через «Маршрут VPN» (колонка «Маршрут»).

А.65.3.18 Перейти в подраздел «Туннели» раздела «Маршруты».

А.65.3.19 Проверить, что активности по туннелю «Маршрут VPN» нет.

А.65.3.20 Подключиться к данному узлу, используя SSH-клиент и данные о доступе, полученные в пункте А.65.3.7. Процедура подключения должна проводиться согласно документу RU.ВАТС.00182-01 32 01 «Специальное программное обеспечение подсистемы ретрансляции данных с использованием промежуточных серверов. Руководство системного программиста».

А.65.3.21 Выполняют команду «ps –ax | grep ‘tor|openvpn|i2p|fhs|prox|socks’» для проверки наличия запущенных процессов маскирования трафика.

A.65.3.22 Выполняют команду «netstat –nltpa | grep ‘tor|openvpn|i2p|fhs|prox|socks’» для отображения списка открытых портов и соединений.

A.65.3.23 Выполнить команду проверки существующих соединений через данный узел от имени суперпользователя: ~~sudo~~ iftop

A.65.3.24 Настроить отображение соединений последовательным нажатием клавиш: sDn

Данная последовательность отключает отображение адреса источника (s), включает отображение портов целевых сервисов (D), отключает отображение доменных имен (n).

A.65.3.25 Проверить наличие маскирующих активных соединений с различными Интернет-сервисами ~~(в т.ч. на порты 80 и 443)~~, не инициируемые со стороны пользователей ПРД, т.к. вся работа через данный маршрут для пользователей была приостановлена.

A.65.3.26 Нажать клавишу «q» для выхода из программы iftop.

A.65.3.27 Проверить общее количество установленных маскирующих tcp-соединений следующей командой от имени суперпользователя:

```
netstat -ntp| wc -l
```

Количество соеденинений должно быть больше 20.

~~A.65.3.28~~

A.65.3.29 В Интерфейсе управления ПРД перейти в раздел «Правила».

A.65.3.30 Разрешить доступ в Интернет пользователям, работающим через «Маршрут VPN».

A.65.3.31 На АРМ пользователя ПРР запустить обозреватель Chromium и открыть ссылку: https://bit.ly/2Jb7jzR.

A.65.3.32 Проверить на выходном узле ретрансляции, что есть подключение к ~~в окне вывода состояния iftop среди маскирующих легитимных подключений отображается подключение к узлу~~ IP-адресу 37.9.96.20. Для этого выполнить команду:

```
netstat -ntp|grep 37.9.96.20
```

A.65.4 СПО ПРД считается выдержавшим испытания по п. A.65.3.1-A.65.3.32 программы и методики испытаний и выполняющим пункты 3.2.6, 3.2.6.8 ТЗ на СЧ ОКР, если:

- при выполнении вышеуказанных действий данной методики отсутствовали сообщения об ошибках;
- был успешно создан дистрибутив для узла;
- была произведена успешная авторизация в интерфейс управления;
- в списке процессов присутствовали tor, i2p, прокси-сервера, openvpn, https веб-сервера;

- в списке открытых портов присутствовали порты для процессов tor (произвольный порт), i2p (произвольный порт), прокси-сервера (произвольный порт), openvpn, https веб-сервера;
- была успешно проведена проверка маскирования запросов пользователей подсистемы ПРД среди запросов сторонних пользователей.

А.66 Методика № 66

А.66.1 В данной методике проводится проверка СПО ПРД на соответствие требованиям пунктов 3.2.6, 3.2.6.9 ТЗ на СЧ ОКР «Амезит-В».

А.66.2 В соответствии с требованиями пунктов 3.2.6, 3.2.6.9 ТЗ на СЧ ОКР «Амезит-В» СПО ПРД должно обеспечивать сокрытие персонализирующей информации прикладного уровня должно контролироваться СПО, устанавливаемым на АРМ оператора. Устанавливаемое СПО должно проверять соответствие локальных настроек пользователя и текущего выходного сетевого адреса пользователя. Проверяемые настройки следующие:

- запрет использования WebRTC в обозревателе пользователя;
- запрет использования в обозревателе пользователя плагинов: Adobe Flash, ActiveX, Java-апплетов;
- временная зона пользователя в системе;
- доступные языковые раскладки в системе.

Администратор должен иметь возможность определять требования к проверяемым настройкам пользователя. В случае несоответствия настроек пользователя – доступ к подсистеме ретрансляции данных должен блокироваться.

Примечание. Должны быть учтены следующие источники персонализирующей информации: обозреватели (при взаимодействии с сервисами ГИС ОП по HTTP, HTTPS, WebRTC, WebDAV, FTP протоколам); почтовые программы; программы мгновенного обмена сообщениями; системное и прикладное программное обеспечение.

А.66.3 Для проведения проверки СПО ПРД на соответствие предъявляемым требованиям необходимо выполнить действия, описанные ниже.

А.66.3.1 Запустить обозреватель и перейти на страницу авторизации интерфейса управления СПО ПРД.

А.66.3.2 Произвести авторизацию в интерфейсе управления с использованием учетных данных системного программиста (администратора).

А.66.3.3 Перейти в раздел «Правила» и выбрать правило «АРМ ПРД».

А.66.3.4 Для всех параметров прикладных настроек установить значение «Запретить» (кроме временной зоны и языковых раскладок).

А.66.3.5 Сохранить изменения параметров пользователя.

А.66.3.6 Открыть новую вкладку обозревателя и открыть страницу: http://ya.ru.

А.66.3.7 Согласно документу RU.ВАТС.00182-01 34 01 «Специальное программное обеспечение подсистемы ретрансляции данных с использованием промежуточных серверов. Руководство оператора» изменить прикладные настройки на АРМ пользователя по рекомендациями СПО КПН.

А.66.3.8 Обновить вкладку обозревателя в соответствии с пунктом А.66.3.6.

А.66.3.9 Открыть общедоступный сервис проверки настроек обозревателя и параметров анонимизации (например, https://2ip.ru/privacy).

А.66.4 СПО ПРД считается выдержавшим испытания по п. А.66.3.1-А.66.3.9 программы и методики испытаний и выполняющим пункты 3.2.6, 3.2.6.9 ТЗ на СЧ ОКР, если:

- при выполнении вышеуказанных действий данной методики отсутствовали сообщения об ошибках;
- была произведена успешная авторизация в интерфейс управления;
- перед изменением прикладных настроек на АРМ пользователя страница не была открыта (доступ к ресурсам ГИС Интернет был заблокирован);
- после изменением прикладных настроек на АРМ пользователя страница была успешно открыта;
- результаты проверки настроек обозревателя и параметров анонимизации соответствовали требования к прикладным настройкам, указанным выше.

А.67 Методика № 67

А.67.1 В данной методике проводится проверка СПО ПРД на соответствие требованиям пунктов 3.2.6, 3.2.6.10 ТЗ на СЧ ОКР «Амезит-В».

А.67.2 В соответствии с требованиями пунктов 3.2.6, 3.2.6.10 ТЗ на СЧ ОКР «Амезит-В» СПО ПРД должно обеспечивать создание виртуальных маршрутов по настраиваемым администратором шаблонам со следующими параметрами:

- длина маршрута (не менее 3 шагов);
- точка входа (диапазон персонализирующих признаков или национальная принадлежность);

- точка выхода (диапазон персонализирующих признаков или национальная принадлежность);

- перечень национальных признаков, соответствующих виртуальному маршруту;

- механизм ретрансляции данных в цепочке между первой и последней точкой виртуального маршрута – tor или vpn.

А.67.3 Для проведения проверки СПО ПРД на соответствие предъявляемым требованиям необходимо выполнить действия, описанные ниже.

А.67.3.1 Запустить обозреватель и перейти на страницу авторизации интерфейса управления СПО ПРД.

А.67.3.2 Произвести авторизацию в интерфейсе управления с использованием учетных данных системного программиста (администратора).

А.67.3.3 Перейти в раздел «Маршруты».

А.67.3.4 Нажать на кнопку «Создать».

А.67.3.5 Выбрать произвольный маршрут с типом VPN.

А.67.3.6 В карточке маршрута для параметра «Прикладные настройки» выбрать значение «Проверять».

А.67.3.7 Активировать панель маршрута «Правила».

А.67.4 СПО ПРД считается выдержавшим испытания по п. А.67.3.1-А.67.3.7 программы и методики испытаний и выполняющим пункты 3.2.6, 3.2.6.10 ТЗ на СЧ ОКР, если:

- при выполнении вышеуказанных действий данной методики отсутствовали сообщения об ошибках;

- при выполнении пп. А.67.3.2 была произведена успешная авторизация в интерфейс управления;

- при выполнении пп. А.67.3.3 в списке маршрутов отображались маршруты типа VPN и Tor;

- при выполнении пп. А.67.3.4 отобразился список типов маршрутов, включающий строки: VPN и TOR;

- при выполнении пп. А.67.3.5 в карточке маршрута присутствовали параметры: «Длина», «Тип»;

- при выполнении пп. А.67.3.6 в карточке маршрута для прикладных настроек предоставлялась возможность настроить требования к: временной зоне, языковым раскладкам и локализации системы;

- при выполнении пп. А.67.3.7 отображались правила выбора узлов ретрансляции данных и предоставлялась возможность изменения следующих критериев выбора узлов: «Страна», «Провайдер», «IP-адрес», «Группа».

A.68 Методика № 68

А.68.1 В данной методике проводится проверка СПО ПРД на соответствие требованиям пунктов 3.2.6, 3.2.6.11 ТЗ на СЧ ОКР «Амезит-В».

А.68.2 В соответствии с требованиями пунктов 3.2.6, 3.2.6.11 ТЗ на СЧ ОКР «Амезит-В» СПО ПРД должно обеспечивать возможность централизованного управления СПО ретрансляции данных (в ручном и автоматизированном режиме): конфигурирование «точек» входа, выхода и промежуточных точек виртуальных транспортных маршрутов ретрансляции данных.

А.68.3 Для проведения проверки СПО ПРД на соответствие предъявляемым требованиям необходимо выполнить действия, описанные ниже.

А.68.3.1 Проверка выполняется в соответствии с методикой № Методика № 67.

А.68.4 СПО ПРД считается выдержавшим испытания по п. А.68.3.1 программы и методики испытаний и выполняющим пункты 3.2.6, 3.2.6.11 ТЗ на СЧ ОКР, если:

- при выполнении вышеуказанных действий данной методики отсутствовали сообщения об ошибках;
- при выполнении пп. А.67.3.2 методики № Методика № 67 была произведена успешная авторизация в интерфейс управления;
- при выполнении пп. А.67.3.7 методики № Методика № 67 была доступна возможность задавать правила для выбора каждой «точки» (узла) для виртуального транспортного маршрута ретрансляции данных типа «VPN»;
- при выполнении пп. А.67.3.7 методики № Методика № 67 была доступна возможность задавать правила выбора входного узла «прикрытия» и выходных правил для виртуальных транспортных маршрутов ретрансляции типа «Tor»;
- при выполнении пп. А.67.3.7 методики № Методика № 67 правила выбора позволяли задавать критерии, определяющие как «множество узлов» (более чем 1 узел, подходящий под критерий правила выбора, например – по стране) для каждой «точки» маршрута, так и конкретные узлы (по IP-адресу);
- при выполнении пп. А.67.3.7 методики № Методика № 67 в карточке маршрута отображалось количество возможных виртуальных транспортных туннелей, удовлетворяющих заданным правилам выбора «точек» ретрансляции в маршруте.

А.69 Методика № 69

А.69.1 В данной методике проводится проверка СПО ПРД на соответствие требованиям пунктов 3.2.6, 3.2.6.12 ТЗ на СЧ ОКР «Амезит-В».

А.69.2 В соответствии с требованиями пунктов 3.2.6, 3.2.6.12 ТЗ на СЧ ОКР «Амезит-В» СПО ПРД должно обеспечивать возможность прогноза скорости передачи данных с использованием виртуального транспортного маршрута.

А.69.3 Для проведения проверки СПО ПРД на соответствие предъявляемым требованиям необходимо выполнить действия, описанные ниже.

А.69.3.1 Запустить обозреватель и перейти на страницу авторизации интерфейса управления СПО ПРД.

А.69.3.2 Произвести авторизацию в интерфейсе управления с использованием учетных данных системного программиста (администратора).

А.69.3.3 Перейти в раздел «Правила».

А.69.3.4 Выбрать правило «Пользователь ПРД».

А.69.3.5 В карточке правила изменить значение параметра «Прикладные настройки» на значение «Не проверять».

А.69.3.6 Указать маршрут «Маршрут VPN».

А.69.3.7 Сохранить изменения правила.

А.69.3.8 Перейти в раздел «Туннели».

А.69.3.9 Выбрать туннель «Маршрут VPN».

А.69.3.10 В карточке туннеля проверить наличие значения «Прогнозируемая скорость».

А.69.3.11 Открыть новую вкладку обозревателя и открыть любой общедоступный сервис тестирования скорости интернет-соединения (например, https://2ip.ru/speed) для определения скоростных характеристик соединения с ГИС Интернет.

А.69.4 СПО ПРД считается выдержавшим испытания по п. А.69.3.1-А.69.3.11 программы и методики испытаний и выполняющим пункты 3.2.6, 3.2.6.12 ТЗ на СЧ ОКР, если:

- при выполнении вышеуказанных действий данной методики отсутствовали сообщения об ошибках;
- при выполнении пп. А.69.3.2 была произведена успешная авторизация в интерфейс управления;
- была успешно отображена прогнозная скорость передачи данных;

- разница между результатами пунктов А.69.3.10 и А.69.3.11 составлялет не более 25 %.

А.70 Методика № 70

А.70.1 В данной методике проводится проверка СПО ПРД на соответствие требованиям пунктов 3.2.6, 3.2.6.13 ТЗ на СЧ ОКР «Амезит-В».

А.70.2 В соответствии с требованиями пунктов 3.2.6, 3.2.6.13 ТЗ на СЧ ОКР «Амезит-В» СПО ПРД должно обеспечивать контроль работоспособности точек виртуальных маршрутов.

А.70.3 Для проведения проверки СПО ПРД на соответствие предъявляемым требованиям необходимо выполнить действия, описанные ниже.

А.70.3.1 Запустить обозреватель и перейти на страницу авторизации интерфейса управления СПО ПРД.

А.70.3.2 Произвести авторизацию в интерфейсе управления с использованием учетных данных системного программиста (администратора).

А.70.3.3 Перейти в раздел «Узлы».

А.70.3.4 Выбрать любой узел ретрансляции с состоянием узла, отображаемым «зеленым индикатором».

А.70.3.5 Записать его IP-адрес и номер узла.

А.70.3.6 Открыть панель «Данные о доступе».

А.70.3.7 Записать данные для доступа по SSH.

А.70.3.8 Оставить открытой вкладку обозревателя.

А.70.3.9 С помощью SSH-клиента, согласно документу RU.BATC.00182-01 32 01 «Специальное программное обеспечение подсистемы ретрансляции данных с использованием промежуточных серверов. Руководство системного программиста», произвести подключение к узлу ретрансляции, используя данные пункта А.70.3.7.

А.70.3.10 Установить на узле ретрансляции tmux. Для узлов ретрансляции на базе ОС Debian установка выполняется командой:

```
sudo apt-get install tmux
```

Для узлов с пакетным менеджером на базе RPM – командой:

```
sudo yum install tmux
```

Установка должна производиться от имени суперпользователя.

А.70.3.11 Запустить tmux, выполнив команду:

```
tmux
```

А.70.3.12 Выполнить следующую команду (от имени суперпользователя):

```
iptables –I INPUT 1 –j DROP; sleep 300; iptables –D INPUT 1
```

А.70.3.13 В обозревателе вернуться к вкладке с узлом ретрансляции (пункт А.70.3.8).

А.70.3.14 Инициировать проверку состояния узла (согласно документу RU.ВАТС.00182-01 92 01 «Специальное программное обеспечение подсистемы ретрансляции данных с использованием промежуточных серверов. Руководство пользователя»).

А.70.3.15 Выполнить повторную проверку состояния узла спустя не менее чем 7 минут.

А.70.4 СПО ПРД считается выдержавшим испытания по п. А.70.3.1-А.70.3.15 программы и методики испытаний и выполняющим пункты 3.2.6, 3.2.6.13 ТЗ на СЧ ОКР, если:

- при выполнении вышеуказанных действий данной методики отсутствовали сообщения об ошибках;
- при выполнении пп. А.70.3.2 была произведена успешная авторизация в интерфейс управления;
- был успешно произведен контроль работоспособоности, состояние узла во время первой проверки было отображено «красным индикатором» (узел недоступен), во время второй проверки «зеленым индикатором» (узел доступен).

А.71 Методика № 71

А.71.1 В данной методике проводится проверка СПО ПРД на соответствие требованиям пунктов 3.2.6, 3.2.6.14 ТЗ на СЧ ОКР «Амезит-В».

А.71.2 В соответствии с требованиями пунктов 3.2.6, 3.2.6.14 ТЗ на СЧ ОКР «Амезит-В» СПО ПРД должно обеспечивать выполнение функций добавления шумовых конструкций в целях статистического камуфлирования данных, проходящих через технические средства ретрансляции данных, под легальные пользовательские запросы к общедоступным сервисам.

А.71.3 Для проведения проверки СПО ПРД на соответствие предъявляемым требованиям необходимо выполнить действия, описанные ниже.

А.71.3.1 Проверка выполняется в ходе действий, проводимых в рамках методики № Методика № 65.

А.71.4 СПО ПРД считается выдержавшим испытания по п. А.71.3.1 программы и методики испытаний и выполняющим пункты 3.2.6, 3.2.6.14 ТЗ на СЧ ОКР при успешном прохождении методики № Методика № 65, так как функция камуфлирования данных, проходящих через узлы ретрансляции

данных, решается запуском на них дополнительного ПО, обеспечивающего генерацию постоянного транзитного трафика. Таким программным обеспечением выступает Tor (в режиме exit-node) и I2P. Кроме этого, VPN сервер запускается в режиме совместного использования порта с https-сервером, что проверяется путем обращения в обозревателе по адресу: https://<IP-адрес-узла-ретрансляции>. При открытии указанного адреса в обозревателе пользователю должна отобразиться html-страница.

A.72 Методика № 72

A.72.1 В данной методике проводится проверка СПО ПРД на соответствие требованиям пунктов 3.2.6, 3.2.6.15 ТЗ на СЧ ОКР «Амезит-В».

A.72.2 В соответствии с требованиями пунктов 3.2.6, 3.2.6.15 ТЗ на СЧ ОКР «Амезит-В» СПО ПРД должно обеспечивать сокрытие истинного назначения группировки точек виртуальных маршрутов путем размещения на них общедоступных ресурсов (требования уточняются по результатам этапа эскизного проектирования).

A.72.3 Для проведения проверки СПО ПРД на соответствие предъявляемым требованиям необходимо выполнить действия, описанные ниже.

A.72.3.1 Проверка выполняется в ходе действий, проводимых в рамках методики № Методика № 65.

A.72.4 СПО ПРД считается выдержавшим испытания по п. A.72.3.1 программы и методики испытаний и выполняющим пункты 3.2.6, 3.2.6.15 ТЗ на СЧ ОКР, если успешно выполнены проверки методики № Методика № 65 в части обеспечения возможности размещения на узлах ретрансляции общедоступных ресурсов следующих типов:

- выходные узлы сети анонимизации Tor;
- маршрутизатор i2p;
- прокси-сервер;
- веб-сервер (может использоваться для маскирования VPN-сервера под https-сервер).

A.73 Методика № 73

A.73.1 В данной методике проводится проверка СПО ПРД на соответствие требованиям пунктов 3.2.6, 3.2.6.16 ТЗ на СЧ ОКР «Амезит-В».

A.73.2 В соответствии с требованиями пунктов 3.2.6, 3.2.6.16 ТЗ на СЧ ОКР «Амезит-В» выполнение требований СПО ретрансляции данных в части СПО мониторинга сети Интернет и «раскрутки» материалов должно

выполняться различными способами и не допускать раскрытия информации при вскрытии одного из них.

А.73.3 Для проведения проверки СПО ПРД на соответствие предъявляемым требованиям необходимо выполнить действия, описанные ниже.

А.73.3.1 Проверка выполняется в ходе испытаний, проводимых согласно методике № Методика № 58 и методике № Методика № 59.

А.73.4 СПО ПРД считается выдержавшим испытания по п. А.73.3.1 программы и методики испытаний и выполняющим пункты 3.2.6, 3.2.6.16 ТЗ на СЧ ОКР при успешном прохождении методики № Методика № 58 и методики № Методика № 59. В указанных методиках проверяется возможность ретрансляции данных с использованием различных типов виртуальных маршрутов (Tor и VPN) в соответствии с настройками, задаваемыми системным программистом.

А.74 Методика № 74

А.74.1 В данной методике проводится проверка СПО ПРД на соответствие требованиям пунктов 3.2.6, 3.2.6.17 ТЗ на СЧ ОКР «Амезит-В».

А.74.2 В соответствии с требованиями пунктов 3.2.6, 3.2.6.17 ТЗ на СЧ ОКР «Амезит-В» технические решения разрабатываемого СПО должны блокировать любые непосредственные взаимодействия технических средств раскрутки материалов и мониторинга сети Интернет в обход системы ретрансляции данных.

А.74.3 Для проведения проверки СПО ПРД на соответствие предъявляемым требованиям необходимо выполнить действия, описанные ниже.

А.74.3.1 Выполнение требований ТЗ обеспечивается способом включения СПО ПРД «в разрыв» канала связи между пользователями СПО ПРР, СПО ПМС и ГИС Интернет.

А.74.4 СПО ПРД считается выдержавшим испытания по п. А.74.3.1 программы и методики испытаний и выполняющим пункты 3.2.6, 3.2.6.17 ТЗ на СЧ ОКР, так как СПО ПРД устанавливается «в разрыв» на канале связи между СПО ПРР, СПО ПМС и ГИС Интернет. В указанной схеме размещения СПО ПРД взаимодействие с ресурсами ГИС Интернет в обход системы ретрансляции невозможно.

А.75 Методика № 75

А.75.1 В данной методике проводится проверка СПО ПРД на соответствие требованиям пунктов 3.2.6, 3.2.6.18 ТЗ на СЧ ОКР «Амезит-В».

А.75.2 В соответствии с требованиями пунктов 3.2.6, 3.2.6.18 ТЗ на СЧ ОКР «Амезит-В» СПО ПРД должно предоставлять шлюз анонимизации, обеспечивающий следующие механизмы сопряжения для других технических средств АПК «Амезит» (в том числе территориально удаленных):

- полное перенаправление трафика клиента по заданным администратором правилам через выбранный механизм анонимизации (VPN или TOR);
- предоставление socks-прокси для каждого доступного выходного узла на шлюзе анонимизации.

Примечания:

1. Должна быть реализована функция блокирования администратором трафика других технических средств при наличии признаков, способных нарушить скрытность работы подсистемы ПРД.
2. К таким признакам относятся:

- персонализирующие атрибуты средств передачи данных (см. п. А.63.2 настоящего документа);
- персонализирующая информация на прикладном уровне (см. п. А.66.2 настоящего документа);
- перечень запрещенных к посещениям ресурсов (должен быть настраиваемым).

3. Должна быть реализована функция своевременного оповещения администратора в случае срабатывания функции блокирования трафика.
4. Должна быть обеспечена возможность подключения к подсистеме ПРД территориально удаленных элементов (в том числе, мобильных компонентов) АПК «Амезит».

А.75.3 Для проведения проверки СПО ПРД на соответствие предъявляемым требованиям необходимо выполнить действия, описанные ниже.

А.75.3.1 Запустить обозреватель и перейти на страницу авторизации интерфейса управления СПО ПРД.

А.75.3.2 Произвести авторизацию в интерфейсе управления с использованием учетных данных системного программиста (администратора).

А.75.3.3 Перейти в раздел «Правила».

А.75.3.4 Выбрать правило «Пользователь ПРД».

А.75.3.5 В карточке правила изменить значение параметра «Прикладные настройки» на «Не проверять».

А.75.3.6 В параметре «Назначенный маршрут» выбрать «Маршрут VPN».

А.75.3.7 Сохранить изменение.

А.75.3.8 Перейти в подраздел «Прокси маршрутов» раздела «Настройки».

А.75.3.9 Записать ссылку в значении параметра: «Список маршрутов».

А.75.3.10 Должен быть выведен список формата: socks5://<proxy-host:proxy-port>,название маршрута, тип маршрута (Tor или VPN), <IP-адрес выходного узла или параметры выбора выходного узла Tor>.

А.75.3.11 Выбрать произвольную запись для маршрута типа VPN из данного списка.

А.75.3.12 Запустить обозреватель Firefox и выполнить следующие действия:

А.75.3.13 Ввести в адресной строке: about:preferences#advanced

А.75.3.14 Перейти на вкладку «Network» и открыть настройки соединения.

А.75.3.15 Выбрать «Manual proxy configuration».

А.75.3.16 В поле «SOCKS Host» ввести proxy-host (пункт А.75.3.11).

А.75.3.17 В поле Port для «SOCKS Host» ввести proxy-port (пункт А.75.3.11).

А.75.3.18 Нажать «ОК».

А.75.3.19 Открыть новую вкладку и ввести: http://myexternalip.com/raw

А.75.3.20 Сравнить выведенный IP-адрес и <IP-адрес выходного узла> (пункт А.75.3.11).

А.75.3.21 Согласно документу RU.BATC.00182-01 92 01 «Специальное программное обеспечение подсистемы ретрансляции данных с использованием промежуточных серверов. Руководство пользователя» выполнить следующие действия в Chrome:

А.75.3.22 Перейти в подраздел «Запрещенные ресурсы» раздела «Настройки».

А.75.3.23 Добавить в список запрещенных ресурсов запись «myexternalip.com».

~~А.75.3.24 Перейти в раздел «Мониторинг».~~

~~А.75.3.25 Проверить наличие в Журнале сообщений о блокировке доступа к «myexternalip.com».~~

А.75.3.26 Проверить блокировку доступа к странице http://myexternalip.com/. Для этого открыть данную страницу в обозревателе Chromium. Должна отобразиться ошибка открытия.

А.75.3.27 Перейти в раздел «Мониторинг» в интерфейсе управление СПО ПРД.

А.75.3.28 Проверить регистрацию события в интерфейсе администратора. В разеделе «мониторинг» в панели «Журнал сообщений» проверить наличие записи о блокировке доступа для «Пользователь ПРД» к ресурсу «myexternalip.com».

А.75.3.29 Перейти в раздел «Настройки».

А.75.3.30 Перейти в подраздел «Запрещенные ресурсы».

А.75.3.31 Удалить из списка запрещенных ресурсов запись «myexternalip.com».

А.75.4 СПО ПРД считается выдержавшим испытания по п. А.75.3.1-А.75.3.31 программы и методики испытаний и выполняющим пункты 3.2.6, 3.2.6.18 ТЗ на СЧ ОКР, если:

- при выполнении вышеуказанных действий данной методики отсутствовали сообщения об ошибках;
- при выполнении пп. А.75.3.2 была произведена успешная авторизация в интерфейс управления;
- при выполнении пп. А.75.3.20 совпали проверяемые IP-адреса;
- при выполнении пп. А.75.3.25 была отображена ошибка открытия страницы после ее добавления в список запрещенных ресурсов;
- при выполнении пп. А.75.3.27 в журнале сообщений присутствовала запись о блокировке доступа.

А.76 Методика № 76

А.76.1 В данной методике проводится проверка СПО ПРД на соответствие требованиям пунктов 3.2.6, 3.2.6.19 ТЗ на СЧ ОКР «Амезит-В».

А.76.2 В соответствии с требованиями пунктов 3.2.6, 3.2.6.19 ТЗ на СЧ ОКР «Амезит-В» СПО ПРД должно выполнять обнаружение и противодействие попыткам запуска специального программного обеспечения в виртуальной среде и под управлением отладчиков.

А.76.3 Для проведения проверки СПО ПРД на соответствие предъявляемым требованиям необходимо выполнить действия, описанные ниже.

А.76.3.1 Запустить обозреватель и перейти на страницу авторизации интерфейса управления СПО ПРД.

А.76.3.2 Произвести авторизацию в интерфейсе управления с использованием учетных данных системного программиста (администратора).

А.76.3.3 Перейти в раздел «Узлы».

А.76.3.4 Выбрать любой узел ретрансляции с состоянием узла, отображаемым «зеленым индикатором».

А.76.3.5 Записать его IP-адрес и номер узла.

А.76.3.6 Открыть панель «Данные о доступе».

~~А.76.3.7~~

А.76.3.8 Записать данные для доступа по SSH.

А.76.3.9 Открыть панель «Активные сервисы».

А.76.3.10 Записать ID-процессов (PID) активных сервисов. Данные защищенны сервисом мониторинга и контроля от управления отладчиками.

А.76.3.11 С помощью SSH-клиента, согласно документу RU.ВАТС.00182-01 32 01 «Специальное программное обеспечение подсистемы ретрансляции данных с использованием промежуточных серверов. Руководство системного программиста», произвести подключение к узлу ретрансляции, используя данные пункта А.76.3.8.

~~А.76.3.12 На узле ретрансляции функционируют два защищенных модуля СПО ПРД:~~

~~– модуль TOTP-авторизации;~~

~~– модуль мониторинга и контроля.~~

~~А.76.3.13 Определить PID процесса модуля TOTP-авторизации (согласно документу RU.ВАТС.00182-01 32 01 «Специальное программное обеспечение подсистемы ретрансляции данных с использованием промежуточных серверов. Руководство системного программиста») – PID1.~~

~~А.76.3.14 Определить PID процесса модуля мониторинга и контроля (согласно документу RU.ВАТС.00182-01 32 01 «Специальное программное обеспечение подсистемы ретрансляции данных с использованием промежуточных серверов. Руководство системного программиста») – PID2.~~

А.76.3.15 Выполнить попытку подключения отладчиком ~~к модулю TOTP-авторизации~~к всем модулям активных сервисов, введя командыу от имени суперпользователя:

```
gdb -p <PID_защищаемого_процесса1>
```

А.76.3.16 Выполнить попытку подключения отладчиком к модулю мониторинга и контроля, введя команду от имени суперпользователя:

```
gdb -p `pidof <PID2>ncs`
```

А.76.3.17 Отключиться от узла ретрансляции, введя команду:

```
exit
```

А.76.3.18 Согласно документу RU.ВАТС.00182-01 32 01 «Специальное программное обеспечение подсистемы ретрансляции данных с использованием промежуточных серверов. Руководство системного программиста» выполнить действия, описанные ниже.

А.76.3.19 Создать установочный пакет узла ретрансляции для произвольного узла ретрансляции в системе.

А.76.3.20 Скопировать полученный пакет на ВМ ПРР (или любую другую виртуальную машину под управлением ОС Debian), выполнив команду на сервере управления:

```
scp <путь к файлу пакета> <имя_пользователя_ВМ>@<IP-адрес виртуальной машины>:/
tmp.
```

А.76.3.21 Подключиться к ВМ ПРР с помощью SSH-клиента (согласно документу RU.ВАТС.00183-01 32 01 «Специальное программное обеспечение подсистемы подготовки, размещения и «раскрутки» специальных материалов. Руководство системного программиста») и запустить пакет узла ретрансляции в соответствии с указаниями по установке модулей СПО ПРД на узле ретрансляции (согласно документу RU.ВАТС.00182-01 32 01 «Специальное программное обеспечение подсистемы ретрансляции данных с использованием промежуточных серверов. Руководство системного программиста»).

А.76.3.22 Результат выполнения команды запуска должен содержать сообщение: VM detected.

А.76.4 СПО ПРД считается выдержавшим испытания по п. А.76.3.1-А.76.3.22 программы и методики испытаний и выполняющим пункты 3.2.6, 3.2.6.19 ТЗ на СЧ ОКР, если:

- при выполнении вышеуказанных действий данной методики отсутствовали сообщения об ошибках;
- при выполнении пп. А.76.3.2 была произведена успешная авторизация в интерфейс управления;
- при выполнении пп. А.76.3.15 отладчик отобразил сообщение о невозможности ~~подключиться к модулю TOTP-авторизации~~подключиться к защищаемым процессам;
- при выполнении пп. А.76.3.16 отладчик отобразил сообщение о невозможности подключиться к модулю мониторинга и контроля;
- при выполнении пп. А.76.3.22 результат выполнения команды содержал сообщение «VM detected».

А.77 Методика № 77

А.77.1 В данной методике проводится проверка СПО ПРД на соответствие требованиям пунктов 3.2.6, 3.2.6.20 ТЗ на СЧ ОКР «Амезит-В».

А.77.2 В соответствии с требованиями пунктов 3.2.6, 3.2.6.20 ТЗ на СЧ ОКР «Амезит-В» СПО ПРД должно обеспечивать контроль состояния группировки точек виртуальных маршрутов, оперативного выявления попыток

получения НСД к ним, нештатных перезагрузок ОС аппаратного обеспечения и иных фактов нарушения информационной безопасности (ИБ) технических средств ретрансляции, в том числе:

- несанкционированный доступ с правами суперпользователя;
- установка дополнительного (вредоносного) ПО;
- реализация атак типа «отказ в обслуживании»;
- попытки исследования алгоритмов СПО (запуск под управлением отладчика, трассировка, установка точек останова, нарушение целостности СПО, запуск под управлением средств виртуализации, смена времени);
- попытки исследования протокола передачи данных (передача некорректных данных соседним узлам виртуального транспортного маршрута, частые обрывы связи или большие задержки при отправке служебных данных);
- установка запрета выступать в роли точки выхода виртуального маршрута.

Примечание. Перечень действий, относящихся к нарушению ИБ технических средств ретрансляции данных, уточняется по результатам эскизного и технического (при необходимости) проектирования и согласовывается с головным исполнителем.

А.77.3 Для проведения проверки СПО ПРД на соответствие предъявляемым требованиям необходимо выполнить действия, описанные ниже.

А.77.3.1 Подготовить стационарное АРМ для имитации узла ретрансляции:

А.77.3.2 Установить ОС Ubuntu 17.04.

А.77.3.3 Установить SSH-сервер, выполнив команду:

```
sudo apt-get install openssh-server
```

А.77.3.4 Установить SMB-сервер командой:

```
sudo apt-get install samba
```

А.77.3.5 Согласно документу RU.ВАТС.00182-01 32 01 «Специальное программное обеспечение подсистемы ретрансляции данных с использованием промежуточных серверов. Руководство системного программиста» установить необходимое ПО для поддержки Intel SGX.

А.77.3.6 Подключить к коммутатору ПРД.

А.77.3.7 Установить статический IP-адрес из подсети сервера управления СПО ПРД.

А.77.3.8 Подключить и настроить GSM-модем для доступа к ресурсам ГИС Интернет.

А.77.3.9 По завершении базовой настройки перезагрузить АРМ без авторизации в системе после перезагрузки.

А.77.3.10 Согласно документу RU.BATC.00182-01 32 01 «Специальное программное обеспечение подсистемы ретрансляции данных с использованием промежуточных серверов. Руководство системного программиста» выполнить следующие действия на мобильном АРМ пользователя СПО ПРД для добавления нового узла:

А.77.3.11 Запустить обозреватель и перейти на страницу авторизации интерфейса управления СПО ПРД.

А.77.3.12 Произвести авторизацию в интерфейсе управления с использованием учетных данных системного программиста (администратора).

А.77.3.13 Перейти в раздел «Узлы».

А.77.3.14 Создать новый узел с названием «Узел М20» и ввести данные стационарного АРМ (IP-адрес необходимо указать для локальной сети).

А.77.3.15 Не закрывать окно обозревателя.

А.77.3.16 Согласно документу RU.BATC.00182-01 32 01 «Специальное программное обеспечение подсистемы ретрансляции данных с использованием промежуточных серверов. Руководство системного программиста» выполнить действия, описанные ниже, на мобильном АРМ пользователя СПО ПРД с целью настройки узла ретрансляции.

А.77.3.17 Запустить SSH-клиент и подключиться к серверу управления СПО ПРД (согласно документу RU.BATC.00182-01 32 01 «Специальное программное обеспечение подсистемы ретрансляции данных с использованием промежуточных серверов. Руководство системного программиста»).

А.77.3.18 Сгенерировать пакет ПО узла ретрансляции для стационарного АРМ.

А.77.3.19 Установить полученный пакет на стационарное АРМ.

А.77.3.20 Переключиться на окно обозревателя.

А.77.3.21 Перейти в раздел «Узлы».

А.77.3.22 Обновить данные по узлу «Узел М20».

А.77.3.23 Убедиться, что индикатор состояния узла отображается зеленым цветом.

А.77.3.24 Перейти в раздел «Данные о доступе».

А.77.3.25 Проверить наличие Onion-имени узла в панели «Данные о доступе».

А.77.3.26 Отключить стационарное АРМ от коммутатора СПО ПРД.

А.77.3.27 Авторизоваться локально (используя клавиатуру) на стационарном АРМ от имени суперпользователя.

А.77.3.28 Попытка локальной авторизации (пункт. А.77.3.25) не должна завершиться успешно.

А.77.3.29 Отключить от стационарного АРМ манипулятор типа «Мышь».

А.77.3.30 Обновить данные по узлу «Узел М20».

А.77.3.31 В течении пяти минут индикатор состояния узла должен отобразиться оранжевым цветом. Перед переходом к указанному цвету индикатор может быть отображен красным цветом.

А.77.3.32 Активировать панель «Журнал событий».

А.77.3.33 Проверить наличие сообщений о следующих событиях:

- изменение оборудования: удалено оборудование <vendorId>:<productId>;
- время последней загрузки системы: Дата и время последней загрузки;
- отключение сетевого интерфейса <название сетевого интерфейса>;
- попытка локального входа от имени root;
- обнаружен неизвестный процесс: ~~samba~~ smbd (PIDs=<один или несколько идентификаторов процесса>).

А.77.3.34 Перейти на панель «Активные сервисы».

А.77.3.35 Найти в списке процесс(ы) «smbd».

А.77.3.36 Идентификаторы процессов должны совпадать с идентификаторами в PIDs пункта А.77.3.33. Состояние процесса(ов) должно быть «Заморожен».

А.77.4 СПО ПРД считается выдержавшим испытания по п. А.77.3.1-А.77.3.36 программы и методики испытаний и выполняющим пункты 3.2.6, 3.2.6.20 ТЗ на СЧ ОКР, если:

- при выполнении вышеуказанных действий данной методики отсутствовали сообщения об ошибках;
- при выполнении пп. А.77.3.12 была произведена успешная авторизация в интерфейс управления;
- при выполнении пп. А.77.3.25 в панели «Данные о доступе» присутстовало Onion-имя узла;
- при выполнении пп. А.77.3.28 была отображена ошибка авторизации;
- после выполнения пп. А.77.3.26 на сервере управления были получены данные о состоянии узла. Переда данных с узла ретрансляции была выполнена через GSM-модем, т.к. других каналов связи с ГИС ОП Интернет на узле ретрансляции не было. Таким образом демонстируется возможность подключения мобильных компонент к подсистеме;
- при выполнении пп. А.77.3.33 на панели «Журнал событий» присутствовали перечисленные в пп. А.77.3.33 события;

- при выполнении пп. А.77.3.35 в списке процессов присутствовал «smbd»;

- при выполнении пп. А.77.3.36 идентификаторы процессов совпадали с индентификаторами пп. А.77.3.33, а состояние процессов было «Заморожен».

А.78 Методика № 78

А.78.1 В данной методике проводится проверка СПО ПРД на соответствие требованиям пунктов 3.2.6, 3.2.6.21 ТЗ на СЧ ОКР «Амезит-В».

А.78.2 В соответствии с требованиями пунктов 3.2.6, 3.2.6.21 ТЗ на СЧ ОКР «Амезит-В» протоколирование действий технических средств ретрансляции данных должно осуществляться на АРМ управления ретрансляции. Не допускается протоколирование действий пользователей АПК «Амезит» на точках виртуальных транспортных маршрутов, находящихся в ГИС ОП, для чего на точках виртуальных транспортных маршрутов СПО не должно производить запись данных на диск после запуска.

Примечания:

1. До этапа ГИ необходимо разработать следующие документы:

- методики закупки выделенных серверов;
- методики по организации технической поддержки выделенных серверов.

2. Арендованные физически выделенные сервера должны обладать следующими характеристиками:

- возможность удаленного управления через консоль с отдельным сетевым адресом;
- скорость сетевого подключения не меньше 100 Мбит/с для сетевых соединений между сервером и клиентом на территории России;
- поддержка технологии Intel SGX компонентами сервера (центральным процессором, материнской платой, bios);
- жесткий диск не менее 64Гб;
- оперативной памяти не менее 8Гб;
- не менее одного публичного IP-адреса.

Сервера, арендуемые на одной территории, должны располагаться на различных хостинг площадках и у различных провайдеров.

Поддержка СПО до 34 арендуемых серверов (Россия – 8 шт., Китай – 6 шт., США – 6 шт., Европа – 6 шт., страны арабского мира – 6 шт., любые другие страны – 2 шт.)

Количество арендуемых серверов 6 шт. (Россия – 2 шт., Китай – 1 шт., США – 1 шт., Европа – 1шт., страны арабского мира – 1 шт.).

Срок аренды серверов – до конца выполнения ОКР плюс один год.

Источник оплаты не должен выдавать национальную принадлежность арендатора.

А.78.3 Для проведения проверки СПО ПРД на соответствие предъявляемым требованиям необходимо выполнить действия, описанные ниже.

А.78.3.1 Запустить обозреватель и перейти на страницу авторизации интерфейса управления СПО ПРД.

А.78.3.2 Произвести авторизацию в интерфейсе управления с использованием учетных данных системного программиста (администратора).

А.78.3.3 Перейти в раздел «Туннели».

А.78.3.4 Выбрать туннель «Маршрут VPN».

А.78.3.5 Из карточки туннеля выписать узлы, входящие в состав маршрута.

А.78.3.6 IP-адреса всех узлов маршрута выписывают в <регулярное выражение поиска IP-адресов узлов ретрансляции>: IP-адрес-входного-узла|IP-адрес-промежуточного-узла-1|…|IP-адрес-выходного-узла.

А.78.3.7 Перейти в раздел «Узлы».

А.78.3.8 Получить данные для доступа по SSH для всех узлов маршрута (пункт А.78.3.5).

А.78.3.9 Перейти в раздел «Правила».

А.78.3.10 Выбрать произвольное правило с активными клиентами и проверяемыми прикладными настройками (в столбце «Прикладные настройки» не должно быть значения «Не проверять»).

А.78.3.11 Проверить наличие записей в панели «Журнал сообщений» и результаты проверок прикладных настроек пользователя в «Истории проверок».

А.78.3.12 Перейти в раздел «Маршруты».

А.78.3.13 Выбрать «Маршрут VPN».

А.78.3.14 Открыть панель «Туннели».

А.78.3.15 Проверить историю создания туннелей по данному маршруту. Должен присутствовать один активный (текущий) туннель и журнал записей по закрытым ранее.

А.78.3.16 Подключиться ко всем узлам ретрансляции по SSH, используя данные, полученные в пункте А.78.3.8. Процедура подключения выполняется согласно документу RU.ВАТС.00182-01 32 01 «Специальное программное обеспечение подсистемы ретрансляции данных с использованием промежуточных серверов. Руководство системного программиста». На каждом

узле ретрансляции выполнить следующие команды проверок от имени суперпользователя:

```
grep -RiE "<регулярное выражение поиска IP-адресов узлов ретрансляции>" /var/log
| grep -v "IP-адрес-узла-к-которому-подключены"
```

А.78.3.17 Проверить, что результат выполнения команды поиска в журналах событий системы не регистрируется IP-адреса цепочки ретрансляции – вывод команды поиска не должен содержать IP-адресов других узлов маршрута ретрансляции.

А.78.3.18 Проверить, что процессы СПО ретрансляции данных не имеют открытых на запись файлов (не протоколируют действия в файловой системе). Для этого выполнить команду от имени суперпользователя:

```
«lsof -a -d 1-999 -p "$(ps -ax | grep -E '[v]pn|[f]hs|[n]cs' | awk '{print
$1;}' | paste -sd ',' -)" / | awk 'NR==1 || $4~/[0-9]+[uw]/'».
```

~~Для отображения файлов, открытых на запись для процессов СПО.~~ **Результат выполнения команды должен** ~~быть пустым~~содержать только одну строку – заголовок вывода.

А.78.4 СПО ПРД считается выдержавшим испытания по п. А.78.3.1-А.78.3.18 программы и методики испытаний и выполняющим пункты 3.2.6, 3.2.6.21 ТЗ на СЧ ОКР, если:

- при выполнении вышеуказанных действий данной методики отсутствовали сообщения об ошибках;
- была произведена успешная авторизация в интерфейс управления;
- были успешно получены данные для доступа по SSH для всех узлов маршрута;
- в панелях «Журнал сообщений» и «История проверок» карточки выбранного правила присутствовали записи;
- в истории создания туннелей по выбранному маршруту присутствовал один активный туннель и список ранее закрытых туннелей;
- поиск IP-адресов узлов маршрута в журналах событий узлов ретрансляции маршрута не показал найденных записей.

А.79 Методика № 79

А.79.1 В данной методике проводится проверка СПО ПРД на соответствие требованиям пунктов 9, 9.12 ТЗ на СЧ ОКР «Амезит-В».

А.79.2 В соответствии с ребованиями пунктов 9, 9.12 ТЗ на СЧ ОКР «Амезит-В» в случае нештатных ситуаций, попыток анализа СПО ретрансляции данных, а также по команде администратора все модули СПО, конфигурационные файлы, входные и выходные данные СПО ретрансляции должны быть уничтожены.

А.79.3 Для проведения проверки СПО ПРД на соответствие предъявляемым требованиям необходимо выполнить действия, описанные ниже.

А.79.3.1 Запустить обозреватель и перейти на страницу авторизации интерфейса управления СПО ПРД.

А.79.3.2 Произвести авторизацию в интерфейсе управления с использованием учетных данных системного программиста (администратора).

А.79.3.3 Перейти в раздел «Узлы».

А.79.3.4 Выбрать любой узел, на котором доступен https-сервер. Наличие https-сервера можно проверить в панели «Активные сервисы» карточки туннеля. В случае отсутствия таких узлов необходимо обратиться к документу RU.ВАТС.00182-01 32 01 «Специальное программное обеспечение подсистемы ретрансляции данных с использованием промежуточных серверов. Руководство системного программиста» для генерации и установки на узле ретрансляции пакета ПО, включающего https веб-сервер.

А.79.3.5 Получить IP-адрес узла и данные для доступа по SSH для узла с работающим https веб-сервером.

А.79.3.6 Подключиться к узлу ретрансляции по SSH (согласно документу RU.ВАТС.00182-01 32 01 «Специальное программное обеспечение подсистемы ретрансляции данных с использованием промежуточных серверов. Руководство системного программиста») с АРМ пользователя ПРД, используя IP-адрес и данные для доступа по SSH для узла с работающим https веб-сервером.

А.79.3.7 В терминале SSH-сессии выполнить следующие команды от имени суперпользователя (root):

```
# получения PID процесса https-сервера
FHS_PID=`ps ax| grep fhs|grep -v fhsgrep|awk '{print $1;}'`
#  получение расположение исполняемого файла FHS_PID
sudo lsof -p $FHS_PID|grep fhs
```

А.79.3.8 Проверить, что вывод содержит путь к вида </fhs> к исполняемому файлу СПО ПРД узла ретрансляции.

А.79.3.9 Проверить, что бинарный исполняемый файл недоступен для получения командой: ls </fhs> /fhs. Должно отобразиться сообщение об отсутствии указанного файла в файловой системе.

А.79.3.10 Проверить, что данный файл в принципе отсутствует в файловой системе, выполнив команду: sudo find / -type f –name fhs. Вывод команды не должен содержать никаких файлов.

А.79.3.11 Проверить, что образ криптоконтейнера СПО ПРД заполнен нулевыми байтами: sudo hexdump -C /dev/mapper/cdisk | head.

А.79.3.12 Проверить, что процесс fhs (HTTPS-сервера комплекта СПО) действительно запущен связан криптоконтейнером, для этого выполняют команды от имени суперпользователя (root)::

```
#получить идентификатор устройства криптоконтейнера
sudo dmsetup ls|grep cdisk
# вывод должен быть вида: cdsisk (<DEV:ID>)
sudo lsof -p `pidof fhs|sed "s/ /,/"`$FHS_PID | grep <DEV,ID>
```

А.79.3.13 Проверить, что непустой вывод последней команды содержит строку вида: </fhs>, где /fhs – путь к файлу fhs (несуществующему)..

~~А.79.3.14 При необходимости повторить проверку данной методики для всех процессов, связанных с криптоконтейнером (всем пакетом СПО узла ретрансляции). Получение списка данных процессов выполняется командой: sudo lsof | grep <DEV,ID>~~

А.79.4 СПО ПРД считается выдержавшим испытания по п. А.79.3.1-А.79.3.14 программы и методики испытаний и выполняющим пункты 9, 9.12 ТЗ на СЧ ОКР, если:

- в результате проверки расположения исполняемых файлов СПО узла ретрансляции – файлов обнаруженно не было;
- в результате проверки содержимого криптоконтейнера – он заполнен нулевыми байтами, т.е. содержимое криптоконтейнера после запуска очищено;
- в файловой системе не были обнаружены файлы СПО узла ретрансляции.

А.80 Методика № 80

А.80.1 В данной методике проводится проверка СПО ПРР на соответствие требованиям пунктов 3.2.7, 3.2.7.1 ТЗ на СЧ ОКР «Амезит-В».

А.80.2 В соответствии с требованиями пунктов 3.2.7, 3.2.7.1 ТЗ на СЧ ОКР «Амезит-В» СПО ПРР должно обеспечивать подготовку специальных материалов (текстовых, графических, видео-, аудиосообщений).

А.80.3 Для проведения проверки СПО ПРР на соответствие предъявляемым требованиям необходимо выполнить действия, описанные ниже.

А.80.3.1 Создать каталог «Материалы» на рабочем столе Windows рабочего места оператора.

А.80.3.2 Проверка механизма подготовки текстовых материалов выполняется в следующем порядке:

А.80.3.2.1 Запустить приложение Writer из пакета офисных программ LibreOffice.

А.80.3.2.2 В открывшемся пустом текстовом документе ввести текст: «Проверка подготовки текстовых материалов с помощью пакета офисных программ».

А.80.3.2.3 В меню «Файл» выбрать пункт «Сохранить как…».

А.80.3.2.4 Выбрать каталог «Материалы» на рабочем столе, созданный в пункте А.80.3.1.

А.80.3.2.5 В поле «Имя файла» ввести «Текстовый материал», в поле «Тип файла» выбрать «Microsoft Word 2007–2013 XML (.docx)».

А.80.3.2.6 Сохранить файл с подготовленным текстовым материалом нажатием на кнопку «Сохранить». (При отображении сообщения «Документ может включать в себя форматирование или содержимое, которое невозможно сохранить в выбранном формате Microsoft Windows 2007–2013 XML» снять выделение с пункта «Спрашивать при сохранении в формате, отличном от ODF или по умолчанию» и нажать на кнопку «Использовать формат Microsoft Windows 2007–2013 XML».

А.80.3.2.7 Закрыть приложение Writer, выбрав пункт «Выйти из LibreOffice» в меню «Файл».

А.80.3.2.8 Запустить приложение Word из пакета офисных программ Microsoft Office.

А.80.3.2.9 Нажать комбинацию клавиш «Ctrl+O».

А.80.3.2.10 В открывшемся диалоговом окне выбора файла перейти в каталог «Материалы» на рабочем столе и выбрать файл «Текстовый материал».

А.80.3.2.11 Нажать на кнопку «Открыть».

А.80.3.2.12 Дополнить текст файла фразой «Проверочная информация».

А.80.3.2.13 Нажать комбинацию клавиш «Ctrl+S».

А.80.3.2.14 Закрыть приложение Microsoft Office Word, нажав комбинацию клавиш «Alt+F4».

А.80.3.2.15 Запустить приложение Adobe Acrobat.

А.80.3.2.16 Выбрать задачу «Создать pdf из файла».

А.80.3.2.17 Выбрать файл «Текстовый материал» в каталоге «Материалы» на рабочем столе и нажать на кнопку «Открыть».

А.80.3.2.18 В меню «Просмотр» выбрать пункт «Инструменты – Редактирование содержимого».

А.80.3.2.19 На открывшейся панели «Редактирование содержимого» выбрать команду «Добавить текст».

А.80.3.2.20 В новой строке открытого файла ввести текст «Проверка подготовки текстовых материалов с помощью Adobe Acrobat».

А.80.3.2.21 В меню «Файл» выбрать пункт «Сохранить как…».

А.80.3.2.22 В открывшемся диалоговом окне перейти в каталог «Материалы» на рабочем столе, созданный в пункте А.80.3.1.

А.80.3.2.23 В поле «Имя файла» ввести «Текстовый материал2», в поле «Тип файла» выбрать «Файлы Adobe PDF».

А.80.3.2.24 Сохранить файл с подготовленным текстовым материалом нажатием на кнопку «Сохранить».

А.80.3.2.25 Закрыть приложение Adobe Acrobat, выбрав пункт «Выход» в меню «Файл».

А.80.3.2.26 Проверка подготовки текстовых материалов считается выполненной, если в каталоге «Материалы» (созданном в пункте А.80.3.1):

- при открытии файла «Текстовый материал.docx» отображается отображается текст «Проверочная информация»;
- при открытии файла «Текстовый материал2.pdf» отображается отображается текст «Проверочная информация».

А.80.3.3 Проверка механизма подготовки графических материалов выполняется в следующем порядке:

А.80.3.3.1 Запустить приложение Adobe Photoshop.

А.80.3.3.2 В меню «Файл» выбрать пункт «Создать…».

А.80.3.3.3 В открывшемся окне на панели «Подробные сведения о стиле» указать:

- имя стиля: Графические данные;
- ширина: 100 Пикселы;
- высота: 100.

А.80.3.3.4 Нажать на кнопку «Создать».

А.80.3.3.5 На панели инструментов выбрать инструмент «Произвольная фигура».

А.80.3.3.6 В выпадающем блоке «Заливка» выбрать желтый цвет.

А.80.3.3.7 В выпадающем блоке «Фигура» выбрать фигуру «Молния».

А.80.3.3.8 В рабочей (белой) области документа нажать левой кнопкой мыши в левом верхнем углу, отпустить кнопку мыши в правом нижнем углу рабочей области.

А.80.3.3.9 В меню «Файл» выбрать пункт «Сохранить как…».

А.80.3.3.10 В открывшемся окне указать путь к каталогу «Материалы» на рабочем столе (созданному в пункте А.80.3.1) и задать:

- имя файла: Графические данные;
- тип файла: JPEG.

А.80.3.3.11 Нажать на кнопку «Сохранить».

А.80.3.3.12 В открывшемся окне «Параметры JPEG» нажать на кнопку «OK».

А.80.3.3.13 Завершить работу с приложением, выбрав пункт «Выход» в меню «Файл» (при отображении сообщения «Сохранить изменения в документе Adobe Photoshop «Графические данные» перед выходом?» нажать на кнопку «Нет»).

А.80.3.3.14 Проверка подготовки графических материалов считается выполненной, если в каталоге «Материалы» (созданном в пункте А.80.3.1) при открытии файла «Графические данные.jpg» отображаются данные, введенные в пунктах А.80.3.3.5–А.80.3.3.8.

А.80.3.4 Проверка механизма подготовки аудиоматериалов выполняется в следующем порядке:

А.80.3.4.1 Запустить приложение Sony Sound Forge Pro.

А.80.3.4.2 В меню «Transport» выбрать пункт «Record» или нажать комбинацию клавиш «Ctrl+R».

А.80.3.4.3 Произнести в микрофон фразу «Проверка подготовки аудиоматериалов с помощью программы сони саунд фордж».

А.80.3.4.4 По завершении фразы нажать на кнопку «Record» или комбинацию клавиш «Ctrl+R».

А.80.3.4.5 В меню «Файл» выбрать пункт «Сохранить как…».

А.80.3.4.6 В открывшемся окне выбрать каталог «Материалы» на рабочем столе (созданный в пункте А.80.3.1) и указать параметры сохранения:

- имя файла: Аудиоданные;
- тип файла: MP3 аудио (*.mp3);
- шаблон: Аудио 128 кбит/с;
- сохранять метаданные в файле: выключить.

А.80.3.4.7 Нажать на кнопку «Сохранить».

А.80.3.4.8 Завершить работу с программой, выбрав пункт «Выход» в меню «Файл».

А.80.3.4.9 Запустить приложение MorphVOX Pro.

А.80.3.4.10 Слева на панели «Голоса» выбрать псевдоним голоса «Woman».

А.80.3.4.11 В меню «MorphVOX» выбрать «Морфинг файла».

А.80.3.4.12 В открывшемся окне выполнить следующие действия:

- в строке «Источник» нажать на кнопку «Обзор» и выбрать из каталога «Материалы» на рабочем столе файл «Аудиоданные.mp3» (созданный в пунктах А.80.3.4.1–А.80.3.4.7);

- в строке «Назначение» нажать на кнопку «Обзор», выбрать каталог «Материалы» на рабочем столе, задать имя файла «Аудиоданные» и тип файла – Wave files (*.wav);
- нажать на кнопку «Сделать»;
- дождаться завершения процесса преобразования;
- нажать на кнопку «Выход».

А.80.3.4.13 Завершить работу с программой, выбрав пункт «Выход» в меню MorphVOX.

А.80.3.4.14 Запустить приложение Voice Converter.

А.80.3.4.15 Дважды нажать левой кнопкой мыши в центральной области окна программы.

А.80.3.4.16 В каталоге «Материалы» на рабочем столе, созданном в пункте А.80.3.1, выбрать файл «Аудиоданные.wav».

А.80.3.4.17 В случае отображения сообщения «This is a stereo sound. Only left channel will be processed» нажать на кнопку «OK».

А.80.3.4.18 В верхнем меню нажать на кнопку «PRESETS» и выбрать из выпадающего списка предустановку «Kid».

А.80.3.4.19 Нажать на кнопку «Apply And Save Conversion» в верхнем меню.

А.80.3.4.20 В открывшемся окне выбрать каталог «Материалы» на рабочем столе, задать имя файла «Аудиоданные2» и нажать на кнопку «Сохранить».

А.80.3.4.21 Дождаться завершения процесса преобразования и записи файла.

А.80.3.4.22 Завершить работу с программой нажатием на кнопку «Закрыть» в правом верхнем углу окна.

А.80.3.4.23 Проверка подготовки аудиоматериалов считается выполненной, если в каталоге «Материалы» (созданном в пункте А.80.3.1):

- при открытии файла «Аудиоданные.wav» воспроизводятся модифицированные аудиоданные в соответствии с псевдонимом голоса, выбранном в пункте А.80.3.4.10;
- при открытии файла «Аудиоданные2.wav» воспроизводятся модифицированные аудиоданные в соответствии с предустановками, выбранными в пункте А.80.3.4.18.

А.80.3.5 Проверка механизма подготовки видеоматериалов выполняется в следующем порядке:

А.80.3.5.1 Запустить приложение Sony Vegas Pro.

А.80.3.5.2 В меню «Файл – Импорт» выбрать пункт «Мультимедиа…».

А.80.3.5.3 В открывшемся окне выбрать каталог «Материалы» на рабочем столе (созданный в пункте А.80.3.1). Удерживая клавишу Ctrl, выделить в нем файлы «Аудиоданные2.wav» и «Графические данные.jpg».

А.80.3.5.4 Нажать на кнопку «Открыть».

А.80.3.5.5 Из панели «Медиафайлы проекта» перетащить на временную шкалу файл «Аудиоданные2.wav».

А.80.3.5.6 Из панели «Медиафайлы проекта» перетащить на временную шкалу файл «Графические данные.jpg».

А.80.3.5.7 Выровнять хронометраж графических данных на временной шкале в соответствии с аудиоданными, переместив правый край графических данных на временной шкале до правого края аудиоданных.

А.80.3.5.8 На панели «Видеоспецэффекты» из древовидного списка выбрать пункт «Новости».

А.80.3.5.9 Перетащить предустановку «Цветная печать» на временную шкалу с графическими данными.

А.80.3.5.10 В открывшемся окне «Спецэффекты видеособытия» в строке «Размер точки» нажать на кнопку «Animate».

А.80.3.5.11 На отобразившейся временной шкале установить позицию курсора на начало временной шкалы и в поле «Размер точки» задать значение 0.

А.80.3.5.12 Установить позицию курсора на конец временной шкалы, нажать на кнопку «Add keyframe» и в поле «Размер точки» задать значение 1.

А.80.3.5.13 Закрыть окно «Спецэффекты видеособытия» кнопкой «Закрыть» в правом верхнем углу окна.

А.80.3.5.14 Выбрать пункт «Визуализировать как…» в меню «Файл».

А.80.3.5.15 В открывшемся окне «Render as» в разделе «Output Format» сохранение в формате MPEG-4 (качество видео в преднастройках выбрать для iPod).

А.80.3.5.16 Нажать на кнопку «Browse».

А.80.3.5.17 Выбрать каталог «Материалы» на рабочем столе (созданный в пункте А.80.3.1), задать имя файла «Видеоданные» и нажать на кнопку «Сохранить».

А.80.3.5.18 Нажать на кнопку «Render».

А.80.3.5.19 Дождаться завершения процесса визуализации, после чего нажать на кнопку «Закрыть» в окне процесса визуализации.

А.80.3.5.20 Завершить работу с программой, выбрав пункт «Выход» в меню «Файл» (при отображении окна с сообщением «Сохранить изменения в Без названия?» нажать на кнопку «Нет»).

А.80.3.5.21 Проверка подготовки видеоматериалов считается выполненной, если в каталоге «Материалы» при открытии файла «Видеоданные.mp4» воспроизводится видеоизображение фигуры «Молния» с воспроизведением фразы «Проверка подготовки аудио материалов с помощью программы сони саунд фордж» в аудиоряде.

А.80.4 СПО ПРР считается выдержавшим испытания по п. А.80.3.1-А.80.3.5.21 программы и методики испытаний и выполняющим пункты 3.2.7, 3.2.7.1 ТЗ на СЧ ОКР, если успешно завершены проверки пунктов А.80.3.2.26, А.80.3.3.14, А.80.3.4.23, А.80.3.5.21.

А.81 Методика № 81

А.81.1 В данной методике проводится проверка СПО ПРР на соответствие требованиям пунктов 3.2.7, 3.2.7.2 ТЗ на СЧ ОКР «Амезит-В».

А.81.2 В соответствии с требованиями пунктов 3.2.7, 3.2.7.2 ТЗ на СЧ ОКР «Амезит-В» скрытие и генерация легендированной персонализирующей информации в специальных материалах должны обеспечиваться очисткой или заполнением метаданных для следующих форматов файлов:

- офисные документы (Microsoft Office Word, OpenOffice Writer, Adobe PDF) в части доступных атрибутов: название, тема, автор, ключевые слова, время создания, время изменения, менеджер, компания, категория, статус, автор последних правок, номер версии, приложение, комментарии, время последней печати;
- графические файлы (JPG, PNG) в части exif-атрибутов (для JPG) и GPS-координат;
- аудиофайлы (mp3) в части ID3 тэгов;
- видеофайлы – модификация времени создания и изменения дорожек.

А.81.3 Для проведения проверки СПО ПРР на соответствие предъявляемым требованиям необходимо выполнить действия, описанные ниже.

А.81.3.1 Запустить СПО «Легенда».

А.81.3.2 Проверка заполнения метаданных в офисных документах выполняется в следующем порядке:

А.81.3.2.1 Нажать на кнопку «Выбрать файл».

А.81.3.2.2 Выбрать на рабочем столе в каталоге «Материалы» (созданном в пункте А.80.3.1) файл «Текстовый материал.docx» (созданный в пунктах А.80.3.2.1–А.80.3.2.6).

А.81.3.2.3 Нажать на кнопку «Открыть».

А.81.3.2.4 Задать следующие параметры в таблице:

- «Название»: тест ПИМ;
- «Тема»: проверка легендирования;
- «Автор»: Пётр Разумовский;
- «Ключевые слова»: ПИМ; легенда;
- «Время создания»: 2000.08.01 10:20:30;
- «Время изменения»: 2000.10.20 01:02:03;
- «Менеджер»: Иванов Иван Иванович;
- «Компания»: Титанум;
- «Категория»: тестовый документ;
- «Статус»: проверено;
- «Автор последних правок»: оператор ПИМ;
- «Номер версии»: 5;
- «Приложение»: блокнот;
- «Комментарии»: тестовый комментарий;
- «Время последней печати»: 2010.01.02 03:04:05.

А.81.3.2.5 Нажать на кнопку «Сохранить изменения».

А.81.3.2.6 Через проводник Windows открыть каталог «Материалы» на рабочем столе.

А.81.3.2.7 Нажать правой кнопкой мыши на значок файла «Текстовый материал.docx» и выбрать из его контекстного меню пункт «Свойства».

А.81.3.2.8 В открывшемся окне «Свойства: Текстовый материал.docx» на вкладке «Подробно» проверить наличие заданных в пункте А.81.3.2.4 значений в метаданных файла.

А.81.3.2.9 Закрыть окно «Свойства: Текстовый материал.docx» нажатием на кнопку «OK».

А.81.3.3 Проверка заполнения метаданных в графических файлах выполняется в следующем порядке:

А.81.3.3.1 Нажать на кнопку «Выбрать файл».

А.81.3.3.2 Выбрать на рабочем столе в каталоге «Материалы» (созданном в пункте А.80.3.1) файл «Графические данные.jpg» (созданный в пунктах А.80.3.3.1–А.80.3.3.12).

А.81.3.3.3 Нажать на кнопку «Открыть».

А.81.3.3.4 Задать следующие параметры в таблице:

- «Комментарии»: LegendCheck;
- «Авторские права»: JPGAuthor
- «Создатель»: JPGCreator;
- «Время съёмки»: 2000.08.01 10:20:30;
- «Изготовитель камеры»: SONY;

- «Модель камеры»: DSC-H300;
- «GPS Широта»: 51;
- «GPS Долгота»: 20;
- «GPS Высота»: 8.

А.81.3.3.5 Нажать на кнопку «Сохранить изменения».

А.81.3.3.6 Через проводник Windows открыть каталог «Материалы» на рабочем столе.

А.81.3.3.7 Нажать правой кнопкой мыши на значок файла «Графические данные.jpg» и выбрать из его контекстного меню пункт «Свойства».

А.81.3.3.8 В открывшемся окне «Свойства: Графические данные.jpg» на вкладке «Подробно» проверить наличие заданных в пункте А.81.3.3.4 значений в метаданных файла.

А.81.3.3.9 Закрыть окно «Свойства: Графические данные.jpg» нажатием на кнопку «OK».

А.81.3.4 Проверка заполнения метаданных в аудиофайлах выполняется в следующем порядке:

А.81.3.4.1 Нажать на кнопку «Выбрать файл».

А.81.3.4.2 Выбрать на рабочем столе в каталоге «Материалы» (созданном в пункте А.80.3.1) файл «Аудиоданные.mp3» (созданный в пунктах А.80.3.4.1–А.80.3.4.7).

А.81.3.4.3 Нажать на кнопку «Открыть».

А.81.3.4.4 Задать следующие параметры в таблице:

- «Название»: тест ПИМ;
- «Исполнитель»: Пётр Разумовский;
- «Альбом»: Неизданный;
- «Год»: 2100;
- «Жанр»: авторская песня.

А.81.3.4.5 Нажать на кнопку «Сохранить изменения».

А.81.3.4.6 Через проводник Windows открыть каталог «Материалы» на рабочем столе.

А.81.3.4.7 Нажать правой кнопкой мыши на значок файла «Аудиоданные.mp3» и выбрать из его контекстного меню пункт «Свойства».

А.81.3.4.8 В открывшемся окне «Свойства: Аудиоданные.mp3» на вкладке «Подробно» проверить наличие заданных в пункте А.81.3.4.4 значений в метаданных файла.

А.81.3.4.9 Закрыть окно «Свойства: Аудиоданные.mp3» нажатием на кнопку «OK».

А.81.3.5 Проверка заполнения метаданных в видеофайлах выполняется в следующем порядке:

А.81.3.5.1 Нажать на кнопку «Выбрать файл».

А.81.3.5.2 Выбрать на рабочем столе в каталоге «Материалы» (созданном в пункте А.80.3.1) файл «Видеоданные. mp4» (созданный в пунктах А.80.3.5.1–А.80.3.5.19).

А.81.3.5.3 Нажать на кнопку «Открыть».

А.81.3.5.4 Задать следующие параметры в таблице:

- «Время создания»: 2000.08.01 10:20:30;
- «Время изменения»: 2000.10.20 01:02:03.

А.81.3.5.5 Нажать на кнопку «Сохранить изменения».

А.81.3.5.6 Через проводник Windows открыть каталог «Материалы» на рабочем столе.

А.81.3.5.7 Нажать правой кнопкой мыши на значок файла «Видеоданные.mp4» и выбрать из его контекстного меню пункт «Свойства».

А.81.3.5.8 В открывшемся окне «Свойства: Видеоданные.mp4» на вкладке «Подробно» проверить наличие заданных в пункте А.81.3.5.4 значений в метаданных файла.

А.81.3.5.9 Закрыть окно «Свойства: Видеоданные.mp4» нажатием на кнопку «ОК».

А.81.3.6 Нажать на кнопку «Выбрать файл».

А.81.3.7 Выбрать на рабочем столе в каталоге «Материалы» (созданном в пункте А.80.3.1) файл «Текстовый материал.docx» (созданный в пунктах А.80.3.2.1–А.80.3.2.6).

А.81.3.8 Нажать на кнопку «Открыть».

А.81.3.9 Нажать на кнопку «Очистить все метаданные».

А.81.3.10 Через проводник Windows открыть каталог «Материалы» на рабочем столе.

А.81.3.11 Нажать правой кнопкой мыши на значок файла «Текстовый материал.docx» и выбрать из его контекстного меню пункт «Свойства».

А.81.3.12 В открывшемся окне «Свойства: Текстовый материал.docx» на вкладке «Подробно» проверить отсутствие персонализирующей информации в метаданных файла.

А.81.3.13 Закрыть окно «Свойства: Текстовый материал.docx» нажатием на кнопку «ОК».

А.81.4 СПО ПРР считается выдержавшим испытания по п. А.81.3.1-А.81.3.13 программы и методики испытаний и выполняющим пункты 3.2.7,

3.2.7.2 ТЗ на СЧ ОКР, если проверки в пунктах А.81.3.2.8, А.81.3.3.8, А.81.3.4.8, А.81.3.5.8, А.81.3.12 выполнены успешно.

А.82 Методика № 82

А.82.1 В данной методике проводится проверка СПО ПРР на соответствие требованиям пунктов 3.2.7, 3.2.7.3 ТЗ на СЧ ОКР «Амезит-В».

А.82.2 В соответствии с требованиями пунктов 3.2.7, 3.2.7.3 ТЗ на СЧ ОКР «Амезит-В» СПО ПРР должно обеспечивать обход ограничений дополнительных параметров приватности в социальных сетях путем автоматизации следующих действий виртуальных пользователей:

- вступления в закрытые группы;
- отправки запросов на добавление пользователей в друзья.

Примечание. Должна быть обеспечена возможность автоматизации процесса создания виртуальных пользователей, отвечающих критериям для выполнения указанных действий.

А.82.3 Для проведения проверки СПО ПРР на соответствие предъявляемым требованиям необходимо выполнить действия, описанные ниже.

А.82.3.1 Запустить веб-обозреватель.

А.82.3.2 Ввести в адресной строке обозревателя адрес веб-интерфейса СПО ПРР и пройти авторизацию в системе.

А.82.3.3 Перейти в раздел «Мероприятия».

А.82.3.4 На панели команд нажать на кнопку «Коллекция».

А.82.3.5 Задать имя «Мероприятия ПИМ» для новой коллекции мероприятий.

А.82.3.6 Проверка вступления виртуальных пользователей в группу выполняется в следующем порядке:

А.82.3.6.1 Находясь в коллекции «Мероприятия ПИМ», нажать на панели команд на кнопку «+ Мероприятие».

А.82.3.6.2 В открывшемся окне задать следующие параметры мероприятия:

- «Название»: ПИМ Вступление в группу;
- «Тип мероприятия»: Типовые действия;
- «Сценарий»: Вступление в группу;
- «Социальные сети»: включить ВКонтакте;
- «Начало»: задать текущее время;
- «Завершение»: задать время на 15 минут больше чем текущее;
- «Сообщества»: выбрать группу «ПИМ Вымышленные»;

- «Адрес»: задать адрес группы для вступления: https://vk.com/urup_group;
- «Количество»: 5.

А.82.3.6.3 Нажать на кнопку «Создать».

А.82.3.6.4 Дождаться завершения создания мероприятия.

А.82.3.6.5 Проверить наличие пользователей из сообщества «ПИМ вымышленные» в подписчиках группы, заданной в пункте А.82.3.6.2.

А.82.3.7 Проверка отправки запросов на добавление пользователей в друзья выполняется в следующем порядке:

А.82.3.7.1 Открыть в веб-обозревателе страницу «https://twitter.com/kotova74».

А.82.3.7.2 Отметить (запомнить или записать) количество читателей.

А.82.3.7.3 Находясь в коллекции «Мероприятия ПИМ», нажать на панели команд на кнопку «+ Мероприятие».

А.82.3.7.4 В открывшемся окне задать следующие параметры мероприятия:

- «Название»: ПИМ Подписка на пользователя;
- «Тип мероприятия»: Типовые действия;
- «Сценарий»: Подписка на пользователя;
- «Социальные сети»: включить Твиттер;
- «Начало»: задать текущее время;
- «Завершение»: задать время на 15 минут больше, чем текущее;
- «Сообщества»: выбрать группу «ПИМ Вымышленные»;
- «Адрес» задать адрес пользователя для добавления в друзья: https://twitter.com/kotova74;
- «Количество»: 5.

А.82.3.7.5 Нажать на кнопку «Сохранить».

А.82.3.7.6 Дождаться завершения создания мероприятия.

А.82.3.7.7 Повторив пункты А.82.3.7.1–А.82.3.7.2, проверить увеличение количества читателей на странице пользователя на значение, заданное в пункте А.82.3.7.4.

А.82.4 СПО ПРР считается выдержавшим испытания по п. А.82.3.1-А.82.3.7.7 программы и методики испытаний и выполняющим пункты 3.2.7, 3.2.7.3 ТЗ на СЧ ОКР, если:

- в части вступления виртуальных пользователей в группу, если пользователи из группы «ПИМ вымышленные» присутствуют в подписчиках группы https://vk.com/urup_group;

- в части отправки запросов на добавление пользователей в друзья, если количество читателей на странице пользователя «https://twitter.com/kotova74» увеличилось на 5.

А.83 Методика № 83

А.83.1 В данной методике проводится проверка СПО ПРР на соответствие требованиям пунктов 3.2.7, 3.2.7.4 ТЗ на СЧ ОКР «Амезит-В».

А.83.2 В соответствии с требованиями пунктов 3.2.7, 3.2.7.4 ТЗ на СЧ ОКР «Амезит-В» СПО ПРР должно обеспечивать автоматизированное размещение специальных материалов в следующих сервисах:

- Twitter;
- LiveJournal;
- Вконтакте;
- Facebook;
- YouTube;
- Одноклассники;
- Instagram;
- BlogSpot.

В указанных социальных сетях должны поддерживаться следующие типы действий виртуальных пользователей:

- Twitter:
- автоматическая регистрация аккаунтов;
- заполнение профилей пользователя: аватар, география, имя пользователя, описание (о себе);
- размещение текстовых публикаций (твитов);
- размещение публикаций с изображениями ;
- размещение комментариев;
- «лайки» (одобрения) к публикациям и комментариям;
- перепечатка публикаций (репосты);
- добавление в друзья (подписки);
- получение и отправка личных сообщений.
- LiveJournal:
- автоматическая регистрация аккаунтов;
- заполнение профилей пользователя: аватар, география, имя пользователя, описание (о себе), интересы;
- размещение текстовых публикаций;
- размещение публикаций с изображениями;
- размещение комментариев;

- «лайки» (одобрения) к публикациям и ком-ментариям;
- перепечатка публикаций;
- добавления в друзья (подписки);
- получение и отправка личных сообщений.
- Вконтакте:
- автоматическая регистрация аккаунтов с подтверждением по SMS;
- заполнение профилей пользователя: аватар, география, имя пользователя, описание (о себе), интересы;
- размещение текстовых публикаций;
- размещение публикаций с изображениями;
- размещение комментариев;
- «лайки» (одобрения) к публикациям и комментариям;
- перепечатка публикаций;
- добавления в друзья;
- вступление в группу;
- получение и отправка личных сообщений.
- Facebook:
- автоматическая регистрация аккаунтов с подтверждением по SMS;
- заполнение профилей пользователя: аватар, география, имя пользователя, описание (о себе), интересы;
- размещение текстовых публикаций;
- размещение публикаций с изображениями;
- размещение комментариев;
- «лайки» (одобрения) к публикациям и комментариям;
- перепечатка публикаций;
- добавление в друзья;
- вступление в группу;
- получение и отправка личных сообщений.
- YouTube:
- автоматическая регистрация аккаунтов с подтверждением по SMS;
- заполнение профилей пользователя: аватар, география, имя пользователя, описание (о себе);
- загрузка видео на свою страницу;
- размещение комментариев;
- «лайки» (одобрения) к видео и комментариям;
- «дизлайки» (неодобрения) к видео и комментариям;
- имитация просмотра авторизованным пользователем;
- подписка на канал.

- Одноклассники:
- автоматическая регистрация аккаунтов с подтверждением по SMS;
- размещение текстовых публикаций;
- размещение публикаций с изображениями;
- размещение комментариев;
- «лайки» (одобрения) к публикациям и комментариям;
- перепечатка публикаций;
- добавление в друзья;
- вступление в группу;
- получение и отправка личных сообщений.
- Instagram:
- автоматическая регистрация аккаунтов с подтверждением по SMS;
- размещение комментариев;
- «лайки» (одобрения) к фотографиям;
- добавление в друзья;
- получение и отправка личных сообщений;
- размещение фотографий на своих страницах.
- BlogSpot:
- автоматическая регистрация аккаунтов;
- размещение текстовых публикаций;
- размещение публикаций с изображениями;
- размещение комментариев;
- добавление в друзья (подписки);
- получение и отправка личных сообщений.
- сервисы мгновенного обмена сообщениями (Telegram, WhatsApp):
- автоматическая регистрация акаунтов;
- заполнение профилей пользователей;
- отправка текстовых сообщений в Telegram и WhatsApp;
- отправка изображений, видео– и аудиоматериалов в Telegram.

Для реализации подтверждения регистрации по SMS, а также задач SMS-рассылок и распространения аудиозаписей через телефонные сети (звонки), должен использоваться программно-аппаратный комплекс мульти-SIM решений Dinstar, включающий: SIM-банк, GSM-шлюз (не менее 4 антенн), локальный SIM-Cloud сервер.

Функция копирования информации профиля должна поддерживается только для поддерживаемых подсистемой социальных сетей.

А.83.3 Для проведения проверки СПО ПРР на соответствие предъявляемым требованиям необходимо выполнить действия, описанные ниже.

А.83.3.1 Запустить веб-обозреватель.

А.83.3.2 Ввести в адресной строке обозревателя адрес веб-интерфейса СПО ПРР и пройти авторизацию в системе.

А.83.3.3 Перейти в раздел «Мероприятия».

А.83.3.4 Слева в списке «Объектов» выбрать коллекцию «Мероприятия ПИМ» (созданную в пункте А.82.3.5).

А.83.3.5 На панели команд нажать на кнопку «+ Мероприятие».

А.83.3.6 В открывшемся окне задать следующие параметры мероприятия:

- «Название»: ПИМ Размещение материалов;
- «Тип мероприятия»: Размещение публикаций;
- «Сценарий»: Размещение публикаций;
- «Социальные сети»: включить Твиттер;
- «Начало»: задать текущее время;
- «Завершение»: задать время на 15 минут больше, чем текущее;
- «Сообщества»: выбрать группу «ПИМ Вымышленные»;
- «Библиотека»: выбрать из библиотеки «ПИМ Публикации» (должна быть создана и наполнена текстовыми материалами в соответствии с руководством пользователя);
- «Количество»: 20;
- «каждое сообщение не более 1 раза»: включить.

А.83.3.7 Нажать на кнопку «Сохранить».

А.83.3.8 Дождаться завершения выполнения мероприятия.

А.83.3.9 Проверить наличие публикаций с текстовым содержимым из библиотеки, заданной в пункте А.83.3.6, на страницах пользователей группы «ПИМ Вымышленные».

А.83.3.10 Проверка перечня доступных действий в соответствующих «Сервисах» выполняется в пунктах А.97.3.1.

А.83.4 СПО ПРР считается выдержавшим испытания по п. А.83.3.1-А.83.3.10 программы и методики испытаний и выполняющим пункты 3.2.7, 3.2.7.4 ТЗ на СЧ ОКР, если:

- на страницах пользователей группы «ПИМ Вымышленные» присутствуют публикации из «Библиотеки»;
- успешно проведена проверка методики запускаются окна обозревателей виртуальных пользователей;.

A.84 Методика № 84

A.84.1 В данной методике проводится проверка СПО ПРР на соответствие требованиям пунктов 3.2.7, 3.2.7.5 ТЗ на СЧ ОКР «Амезит-В».

A.84.2 В соответствии с требованиями пунктов 3.2.7, 3.2.7.5 ТЗ на СЧ ОКР «Амезит-В» должны быть обеспечены следующие средства поднятия рейтингов распространяемых специальных материалов:

- автоматизированная накрутка счетчиков одобрений (лайков) и перепечаток (репостов) для задаваемых пользователем публикаций ;
- выявление ключевых слов (хештегов), соответствующих заданному пользователем тексту.

Примечания:

1. Должна быть обеспечена возможность автоматизации перепечаток исходных материалов в другие социальные сети
2. Автоматизация действий должна осуществляться с учетом «Методики повышения эффективности распространения специальных и контрпропагандистских материалов, согласованной с головным исполнителем (см. п. 13.3.9 ТЗ).

A.84.3 Для проведения проверки СПО ПРР на соответствие предъявляемым требованиям необходимо выполнить действия, описанные ниже.

A.84.3.1 Запустить обозреватель.

A.84.3.2 Ввести в адресной строке обозревателя адрес веб-интерфейса СПО ПРР и пройти авторизацию в системе.

A.84.3.3 Проверка выполнения автоматизированной накрутки счетчиков одобрений (лайков) и перепечаток (репостов) для задаваемых пользователем публикаций выполняется в следующем порядке:

A.84.3.3.1 Перейти в раздел «Мероприятия».

A.84.3.3.2 Слева в списке «Объектов» выбрать коллекцию «Мероприятия ПИМ» (созданную в пункте A.82.3.5).

A.84.3.3.3 На панели команд нажать на кнопку «+ Мероприятие».

A.84.3.3.4 В открывшемся окне задать следующие параметры мероприятия:

- «Название»: ПИМ Поднятие рейтинга;
- «Тип мероприятия»: Типовые действия;
- «Сценарий»: Одобрение публикации и перепечатка;
- «Социальные сети»: Твиттер;
- «Начало»: задать текущее время;
- «Завершение»: задают время на 15 минут больше, чем текущее;

- «Сообщества»: выбрать группу «ПИМ Вымышленные»;
- «Адрес»: задать адрес любой публикации из результатов, полученных в пункте А.83.3.9;
- «Одобрения»: 3;
- «Перепечатки»: 5.

А.84.3.3.5 Нажать на кнопку «Сохранить».

А.84.3.3.6 Дождаться завершения выполнения мероприятия.

А.84.3.4 Проверка выявления ключевых слов (хештегов), соответствующих заданному пользователем тексту выполняется в следующем порядке:

А.84.3.4.1 Перейти в раздел «Библиотеки».

А.84.3.4.2 Слева в списке «Библиотек» выбрать подраздел «Сообщения».

А.84.3.4.3 Перейти в любую непустую библиотеку.

А.84.3.4.4 Наветси курсор на заголовок любого сообщения с текстом не менее десяти слов.

А.84.3.4.5 Нажать в заголовке сообщения на отобразившуюся кнопку «#».

А.84.3.4.6 В открывшемся модальном окне «Рекомендация хештегов» ввести значение: «Количество хештегов»: 5.

А.84.3.4.7 Нажать на кнопку «Анализ».

А.84.3.4.8 Дождаться завершение анализа.

А.84.3.4.9 Нажать на кнопку «Сохранить».

А.84.3.4.10 Навести курсор на заголовок сообщения, для которого производился анализ, и нажать на отобразившуюся кнопку редактирования.

А.84.4 СПО ПРР считается выдержавшим испытания по п. А.84.3.1-А.84.3.4.10 программы и методики испытаний и выполняющим пункты 3.2.7, 3.2.7.5 ТЗ на СЧ ОКР, если:
- в окне редактирования сообщения присутствуют рекомендованные хештеги;
- на странице целевой публикации присутствует информация о наличии одобрений и перепечаток публикации от пользователей группы «ПИМ Вымышленные».

А.85 Методика № 85

А.85.1 В данной методике проводится проверка СПО ПРР на соответствие требованиям пунктов 3.2.7, 3.2.7.6 ТЗ на СЧ ОКР «Амезит-В».

А.85.2 В соответствии с требованиями пунктов 3.2.7, 3.2.7.6 ТЗ на СЧ ОКР «Амезит-В» СПО ПРР должно обеспечивать автоматизированную регистрацию учетных записей пользователей с использованием генерируемых (с учетом технологий социальной инженерии) личных данных: имя, фамилия, дата рождения, место проживания, интересы, а также фотографии.

А.85.3 Для проведения проверки СПО ПРР на соответствие предъявляемым требованиям необходимо выполнить действия, описанные ниже.

А.85.3.1 Запустить веб-обозреватель.

А.85.3.2 Ввести в адресной строке обозревателя адрес веб-интерфейса СПО ПРР и пройти авторизацию в системе.

А.85.3.3 Перейти в раздел «Пользователи».

А.85.3.4 На панели команд нажать на кнопку «Регистрация».

А.85.3.5 В открывшемся окне указать следующие данные:

- «Название»: ПИМ Вымышленные;
- «Описание»: регистрация с вымышленными данными;
- «Количество пользователей»: 5;
- «Сервисы»: «Twitter», «ВКонтакте» и «Одноклассники»;
- «Почтовые ящики для подтверждения»: Mail.ru;
- «Тип регистрации»: вымышленные данные;
- «Пол»: только женщины;
- «Возраст»: от 18 до 24;
- «Библиотеки аватаров»: «Студентки»;
- «Библиотеки имен»: «Женские имена (рус.)»;
- «Библиотеки имен»: «Женские фамилии (рус.)»;
- «Библиотеки интересов»: «Студентки», «Медики»;
- «Библиотеки описаний»: «Женские», «Кулинария»;
- «Библиотеки геоданных»: «Россия».

А.85.3.6 Нажать на кнопку «+Создать» для запуска задачи автоматизированной регистрации учетных записей пользователей.

А.85.3.7 Дождаться завершения задачи регистрации не менее, чем для одного пользователя не менее чем в одной социальной сети.

Примечание. Индикатор задачи регистрации отображается в подразделе «Регистрации» в столбце «Выполнение». После выполнения генерации профилей виртуальных пользователей количество зарегистрированных пользователей отображается в этом столбце в строке «ПИМ Вымышленные» в формате «Регистрация ботов 5(<X>)», где <X> – количество фактически зарегистрированных пользователей.

А.85.3.8 Перейти в раздел «Пользователи».

А.85.3.9 Слева в списке «Объектов» нажать на строку с сообществом «Регистрация Вымышленные».

А.85.3.10 Выбрав произвольного пользователя в рабочей области, проверить, что данные в профиле пользователя и зарегистрированные сервисы соответствуют данным, указанным в пункте А.85.3.5.

А.85.4 СПО ПРР считается выдержавшим испытания по п. А.85.3.1-А.85.3.10 программы и методики испытаний и выполняющим пункты 3.2.7, 3.2.7.6 ТЗ на СЧ ОКР, если пункт А.85.3.10 выполнен успешно.

А.86 Методика № 86

А.86.1 В данной методике проводится проверка СПО ПРР на соответствие требованиям пунктов 3.2.7, 3.2.7.7 ТЗ на СЧ ОКР «Амезит-В».

А.86.2 В соответствии с требованиями пунктов 3.2.7, 3.2.7.7 ТЗ на СЧ ОКР «Амезит-В» СПО ПРР должно обеспечивать создание копии профиля реально существующего субъекта.

А.86.3 Для проведения проверки СПО ПРР на соответствие предъявляемым требованиям необходимо выполнить действия, описанные ниже.

А.86.3.1 Запустить веб-обозреватель.

А.86.3.2 Ввести в адресной строке обозревателя адрес веб-интерфейса СПО ПРР и пройти авторизацию в системе.

А.86.3.3 Перейти в раздел «Пользователи».

А.86.3.4 На панели команд нажать на кнопку «Регистрация».

А.86.3.5 В открывшемся окне указать следующие данные:

- «Название»: Регистрация Реальные;
- «Описание»: регистрация с реальными данными;
- «Количество»: 2;
- «Сервисы»: «Twitter», «ВКонтакте»;
- «Почтовые ящики»: Yandex;
- «Тип регистрации»: реальные профили;
- «Адреса профилей»: адреса (разделённые переводом строки):
- https://vk.com/gassiev_murat;
- https://twitter.com/kotova74.

А.86.3.6 Нажать на кнопку «+Создать» для запуска задачи автоматизированной регистрации учетных записей пользователей.

А.86.3.7 Дождаться завершения задачи регистрации не менее одного пользователя не менее чем в одной социальной сети.

А.86.3.8 Перейти в раздел «Пользователи».

А.86.3.9 Слева в списке «Объектов» нажать на строку с группой «Регистрация Реальные».

А.86.3.10 Нажать на аватары пользователей в рабочей области, проверить, что данные в профилях пользователей соответствуют данным реальных профилей, указанным в пункте А.86.3.5.

А.86.4 СПО ПРР считается выдержавшим испытания по п. А.86.3.1-А.86.3.10 программы и методики испытаний и выполняющим пункты 3.2.7, 3.2.7.7 ТЗ на СЧ ОКР, если пункт А.86.3.10 выполнен успешно.

А.87 Методика № 87

А.87.1 В данной методике проводится проверка СПО ПРР на соответствие требованиям пунктов 3.2.7, 3.2.7.8 ТЗ на СЧ ОКР «Амезит-В».

А.87.2 В соответствии с требованиями пунктов 3.2.7, 3.2.7.8 ТЗ на СЧ ОКР «Амезит-В» СПО ПРР должно обеспечивать поддержку не менее 100 профилей пользователей социальных сетей с одного рабочего места.

А.87.3 Для проведения проверки СПО ПРР на соответствие предъявляемым требованиям необходимо выполнить действия, описанные ниже.

А.87.3.1 Запустить обозреватель.

А.87.3.2 Ввести в адресной строке обозревателя адрес веб-интерфейса СПО ПРР и пройти авторизацию в системе.

А.87.3.3 Перейти в раздел «Пользователи».

А.87.3.4 Подсчитать в списке «Объектов» суммарное количество виртуальных пользователей, указанное справа от названия сообщества.

А.87.4 СПО ПРР считается выдержавшим испытания по п. А.87.3.1-А.87.3.4 программы и методики испытаний и выполняющим пункты 3.2.7, 3.2.7.8 ТЗ на СЧ ОКР, если общее количество поддерживаемых в СПО пользователей, полученное в пункте А.87.3.4, превышает 100.

А.88 Методика № 88

А.88.1 В данной методике проводится проверка СПО ПРР на соответствие требованиям пунктов 3.2.7, 3.2.7.9 ТЗ на СЧ ОКР «Амезит-В».

А.88.2 В соответствии с требованиями пунктов 3.2.7, 3.2.7.9 ТЗ на СЧ ОКР «Амезит-В» СПО ПРР должно обеспечивать автоматизированную подготовка электронной почты (Yandex, Mail.ru, Gmail) при регистрации учетных записей в поддерживаемых сервисах.

П р и м е ч а н и е. Должны быть реализованы меры по предотвращению несанкционированного доступа к учетным записям.

А.88.3 Для проведения проверки СПО ПРР на соответствие предъявляемым требованиям необходимо выполнить действия, описанные ниже.

А.88.3.1 Запустить обозреватель.

А.88.3.2 Ввести в адресной строке обозревателя адрес веб-интерфейса СПО ПРР и пройти авторизацию в системе.

А.88.3.3 Методика проводится с использованием результатов методики Методика № 85.

А.88.3.4 Перейти в раздел «Пользователи».

А.88.3.5 Слева в списке «Объектов» нажать на строку с сообществом «ПИМ Вымышленные».

А.88.3.6 Нажать на аватары пользователей в рабочей области, проверить, что зарегистрированные сервисы в профилях пользователей соответствуют данным задачи регистрации.

А.88.3.7 На уровне сообщества пользователей «ПИМ Вымышленные» нажать в рабочей области на имя любого пользователя в столбце «Пользователи» для перехода к окну с информацией об имеющихся аккаунтах выбранного пользователя.

А.88.3.8 Проверить, что выполняются нижеследующие правила для сгенерированных СПО паролей аккаунтов, препятствующие несанкционированному доступу к созданным учетным записям:

- длина паролей не менее 10 символов;
- в паролях одновременно используются символы верхнего и нижнего регистров;
- в паролях присутствуют спецсимволы и/или цифры.

А.88.4 СПО ПРР считается выдержавшим испытания по п. А.88.3.1-А.88.3.8 программы и методики испытаний и выполняющим пункты 3.2.7, 3.2.7.9 ТЗ на СЧ ОКР, если выполнена регистрация электронной почты и выполняются нижеследующие правила для сгенерированных СПО паролей аккаунтов, препятствующие несанкционированному доступу к созданным учётным записям:

- длина паролей не менее 10 символов;
- в паролях одновременно используются символы верхнего и нижнего регистров;
- в паролях присутствуют спецсимволы и/или цифры.

А.89 Методика № 89

А.89.1 В данной методике проводится проверка СПО ПРР на соответствие требованиям пунктов 3.2.7, 3.2.7.10 ТЗ на СЧ ОКР «Амезит-В».

А.89.2 В соответствии с требованиями пунктов 3.2.7, 3.2.7.10 ТЗ на СЧ ОКР «Амезит-В» СПО ПРР должно обеспечивать подготовку, хранение и представление оператору профиля виртуального пользователя: личные данные, имеющиеся учетные записи в поддерживаемых сервисах, история действий, личные диалоги в имеющихся учетных записях.

Примечания:

1. Должна быть обеспечена возможность добавления, редактирования и удаления комментариев оператора АПК.
2. Должна быть обеспечения возможность настройки отображения списка профилей виртуальных пользований (группировка аккаунтов одного профиля, группировка профилей, сортировка, фильтры по возрасту, языкам, интересам, национальности и т.д.).

А.89.3 Для проведения проверки СПО ПРР на соответствие предъявляемым требованиям необходимо выполнить действия, описанные ниже.

А.89.3.1 В адресной строке ввести обозревателя адрес веб-интерфейса СПО ПРР и проходят авторизацию в системе.

А.89.3.2 Методика проводится с использованием результатов методики Методика № 86.

А.89.3.3 Перейти в раздел «Пользователи».

А.89.3.4 Слева в списке «Объектов» нажать на строку с сообществом «Регистрация Реальные».

А.89.3.5 В верхней части меню объектов нажать на кнопку фильтров. В открывшейся панели фильтров ввести следующие данные: «Описание пользователя (о себе)»: боксер.

А.89.3.6 Нажать на кнопку «Enter».

А.89.3.7 Убедиться, что в рабочей области справа отображён пользователь «Мурат Гассиев».

А.89.3.8 В верхней части рабочей области справа от названия сообщества пользователей нажать левой кнопкой мыши и в активировавшемся поле ввода вести текст: «проверка ввода произвольного комментария к сообществу».

А.89.3.9 Слева в списке «Объектов» навести курсор на строку с сообществом «Регистрация Реальные» и убедиться, что комментарий оператора также отображается в качестве всплывающей подсказки к сообществу.

А.89.3.10 В верхней части рабочей области справа от названия сообщества пользователей нажать левой кнопкой мыши на комментарии «проверка ввода произвольного комментария к группе».

А.89.3.11 Очистить поле ввода от комментария.

А.89.3.12 Слева в списке «Объектов» навести курсор на строку с сообществом «Регистрация Реальные» и убедиться, что комментарий оператора успешно удалён.

А.89.3.13 В рабочей области нажать на названии столбца «Пользователь»: убедиться, что выполнена сортировка списка по именам пользователей.

А.89.3.14 Просмотреть данные в профилях пользователей, нажав на аватары пользователей.

А.89.3.15 Убедиться, что отображаемые данные пользователя содержат: изображение (аватар), имя, фамилию, интересы, описание, возраст (дату рождения).

А.89.3.16 Нажать на ссылку в столбце «Пользователь» любого виртуального пользователя и перейти к списку его аккаунтов.

А.89.3.17 Убедиться, что для выбранного пользователя отображается список его аккаунтов.

А.89.3.18 В панели команд нажать на кнопку «Задачи». В правом верхнем углу рабочей области выбрать тип отображаемых задач «Планируемые» и нажать на кнопку «Просмотр» для любой из задач.

А.89.3.19 Убедиться, что параметры задач содержат логин и пароль какой-либо из учётных записей просматриваемого пользователя. Нажать на кнопку «Закрыть».

А.89.3.20 В панели команд нажать на кнопку «Диалоги».

А.89.3.21 Убедиться, что отобразился список диалогов с личными сообщениями для данного пользователя.

А.89.4 СПО ПРР считается выдержавшим испытания по п. А.89.3.1-А.89.3.21 программы и методики испытаний и выполняющим пункты 3.2.7, 3.2.7.10 ТЗ на СЧ ОКР, если:

- данные профилей пользователей имеют информативное представление и соответствуют заданным фильтрам;
- для выбранного пользователя отображается список его аккаунтов;
- для выбранного пользователя отображается список его личных сообщений (диалогов).

А.90 Методика № 90

А.90.1 В данной методике проводится проверка СПО ПРР на соответствие требованиям пунктов 3.2.7, 3.2.7.11 ТЗ на СЧ ОКР «Амезит-В».

А.90.2 В соответствии с требованиями пунктов 3.2.7, 3.2.7.11 ТЗ на СЧ ОКР «Амезит-В» СПО ПРР должно обеспечивать анализ и генерацию отчетов о внешней по отношению к профилю активности, включающих:

- полученные личные сообщения и их количество;
- количество добавившихся подписчиков (друзей);
- упоминания другими пользователями и их количество (при наличии технической возможности);
- комментарии и репосты к публикациям профиля, а также их количество;
- рекомендации по повышению эффективности распространения специальных материалов (см. п. А.84.2 настоящего документа).

Примечание. Анализ и генерация отчетов должны выполняться в следующих режимах:

- по запросу пользователя – в заданном интервале времени с уведомлением пользователя о готовности отчета;
- в режиме времени близком к реальному по заранее определенному набору параметров.

А.90.3 Для проведения проверки СПО ПРР на соответствие предъявляемым требованиям необходимо выполнить действия, описанные ниже.

А.90.3.1 Запустить обозреватель.

А.90.3.2 Ввести в адресной строке обозревателя адрес веб-интерфейса СПО ПРР и пройти авторизацию в системе.

А.90.3.3 Перейти в раздел «Пользователи».

А.90.3.4 Слева на панели «Объектов» выбрать сообщество «ПИМ Вымышленные».

А.90.3.5 В рабочей области раздела выбрать произвольного пользователя.

А.90.3.6 На панели команд нажать на кнопку «Отчет».

А.90.3.7 В открывшемся диалоговом окне установить значения:

- «Временной период»: выбрать значение «Весь период»;
- «Сервис»: выбрать «Твиттер»;
- установить в положение «Вкл» переключатели: «Личные сообщения», «Подписчики», «Упоминания», «Комментарии», «Перепечатки», «Одобрения», «Рекомендации».

А.90.3.8 Нажать на кнопку «Создать».

А.90.3.9 Дождаться завершения формирования отчета (этап формирования отображается в текущем модальном окне).

А.90.3.10 Нажать на кнопку «Сохранить».

А.90.3.11 Открыть сохраненный файл.

А.90.4 СПО ПРР считается выдержавшим испытания по п. А.90.3.1-А.90.3.11 программы и методики испытаний и выполняющим пункты 3.2.7, 3.2.7.11 ТЗ на СЧ ОКР, если в открывшемся документе отображается:

- информация об учетной записи, для которой сгенерирован отчет;
- временной интервал, за который были собраны данные для отчета;
- таблица, содержащая счетчики: «Личные сообщения», «Подписчики», «Упоминания», «Комментарии», «Перепечатки», «Одобрения», «Рекомендации»;
- раздел «Личные сообщения», содержащий текст и отправителей полученных личных сообщений за указанный интервал или текст «Личных сообщений получено не было»;
- раздел «Упоминания», содержащий сообщения с упоминаниями данного пользователя или текст «Упоминаний не найдено»;
- раздел «Комментарии», содержащий полученные комментарии к публикациям пользователя или сообщения «Комментариев не найдено»;
- раздел «Рекомендации», содержащий рекомендации по увеличению рейтинга данного пользователя в социальной сети. Например, «У данного пользователя отсутствуют комментарии и одобрения публикаций, рекомендуется увеличить количество подписчиков для данного пользователя».

А.91 Методика № 91

А.91.1 В данной методике проводится проверка СПО ПРР на соответствие требованиям пунктов 3.2.7, 3.2.7.12 ТЗ на СЧ ОКР «Амезит-В».

А.91.2 В соответствии с требованиями пунктов 3.2.7, 3.2.7.12 ТЗ на СЧ ОКР «Амезит-В» СПО ПРР должно обеспечивать распространение информационных сообщений абонентам ГИС ОП посредством электронной почты.

А.91.3 Для проведения проверки СПО ПРР на соответствие предъявляемым требованиям необходимо выполнить действия, описанные ниже.

А.91.3.1 Запустить обозреватель.

А.91.3.2 Ввести в адресной строке обозревателя адрес веб-интерфейса СПО ПРР и пройти авторизацию в системе.

А.91.3.3 Перейти в раздел «Мероприятия».

А.91.3.4 Слева в списке «Объектов» выбрать коллекцию «Мероприятия ПИМ» (созданную в пункте А.82.3.5).

А.91.3.5 На панели команд нажать на кнопку «+ Мероприятие».

А.91.3.6 В открывшемся окне задать следующие параметры мероприятия:

- «Название»: ПИМ Размещение материалов;
- «Тип мероприятия»: Распространение материалов;
- «Сценарий»: Рассылка электронных писем;
- «Начало»: задать текущее время;
- «Завершение»: задать время через 20 минут от текущего;
- «Сообщества»: выбрать группу «ПИМ Вымышленные»;
- «Библиотека»: выбрать из библиотеки «ПИМ Публикации» (должна быть создана и наполнена текстовыми материалами в соответствии с документом RU.BATC.00183-01 92 01 «Специальное программное обеспечение подсистемы подготовки, размещения и «раскрутки» специальных материалов. Руководство пользователя»);
- «Писем получателю»: 20;
- «Уникальные сообщения»: отметить;
- «Получатели»: указать адрес электронной почты произвольного виртуального пользователя из сообщества «ПИМ Вымышленные».

А.91.3.7 Нажать на кнопку «Сохранить».

А.91.3.8 Дождаться завершения создания мероприятия.

А.91.3.9 Используя учетные данные электронной почты виртуального пользователя, выбранного в качестве получателя писем, войти в электронную почту виртуального пользователя (используя веб-обозреватель), перейти в папку «Входящие» и проверить наличие новых писем, отправленных в рамках проведения мероприятия пункта А.91.3.6.

А.91.4 СПО ПРР считается выдержавшим испытания по п. А.91.3.1-А.91.3.9 программы и методики испытаний и выполняющим пункты 3.2.7, 3.2.7.12 ТЗ на СЧ ОКР, если в почтовом ящике пользователя присутствуют электронные письма, отправленные во время проведения мероприятия и их содержимое соответствует отправленным данным.

А.92 Методика № 92

А.92.1 В данной методике проводится проверка СПО ПРР на соответствие требованиям пунктов 3.2.7, 3.2.7.13 ТЗ на СЧ ОКР «Амезит-В».

А.92.2 В соответствии с требованиями пунктов 3.2.7, 3.2.7.13 ТЗ на СЧ ОКР «Амезит-В» СПО ПРР должно обеспечивать распространение информационных сообщений абонентам ГИС ОП через автоматизированную рассылку личных сообщений в поддерживаемых сервисах.

А.92.3 Для проведения проверки СПО ПРР на соответствие предъявляемым требованиям необходимо выполнить действия, описанные ниже.

А.92.3.1 Запустить обозреватель.

А.92.3.2 Ввести в адресной строке обозревателя адрес веб-интерфейса СПО ПРР и пройти авторизацию в системе.

А.92.3.3 Перейти в раздел «Мероприятия».

А.92.3.4 Слева в списке «Объектов» выбрать коллекцию «Мероприятия ПИМ» (созданную в пункте А.82.3.5).

А.92.3.5 На панели команд нажать на кнопку «+ Мероприятие».

А.92.3.6 В открывшемся окне задать следующие параметры мероприятия:

- «Название»: ПИМ Сообщения абонентам;
- «Тип мероприятия»: Типовые действия;
- «Сценарий»: Отправка личных сообщений;
- «Социальные сети»: отметить Твиттер;
- «Начало»: задать текущее время;
- «Завершение»: задать время через 20 минут от текущего;
- «Сообщества»: выбрать сообщество «ПИМ Вымышленные»;
- «Получатели» задать (разделенные переводом строки) идентификаторы произвольных пользователей в заданной социальной сети из сообщества «ПИМ Вымышленные»;
- «Сообщения»: выбрать из библиотеки «ПИМ Сообщения»;
- «Количество от»: 1;
- «Количество до»: 5.

А.92.3.7 Нажать на кнопку «Сохранить».

А.92.3.8 Дождаться завершения создания мероприятия.

А.92.3.9 Войти в социальную сеть Твиттер, используя учетные данные пользователя, заданного как «Получатель» в пункте А.92.3.6, перейти в раздел личных сообщений и проверить наличие входящих личных сообщений из библиотеки «ПИМ Сообщения».

А.92.3.10 Повторить данную методику для каждой из социальных сетей, задаваемых параметром «Социальные сети» мероприятия.

А.92.4 СПО ПРР считается выдержавшим испытания по п. А.92.3.1-А.92.3.9 программы и методики испытаний и выполняющим пункты 3.2.7, 3.2.7.13 ТЗ на СЧ ОКР, если сообщения из библиотеки «ПИМ Сообщения», присутствуют в личных сообщениях получателей социальной сети, задаваемых при проведении мероприятий.

А.93 Методика № 93

А.93.1 В данной методике проводится проверка СПО ПРР на соответствие требованиям пунктов 3.2.7, 3.2.7.14 ТЗ на СЧ ОКР «Амезит-В».

А.93.2 В соответствии с требованиями пунктов 3.2.7, 3.2.7.14 ТЗ на СЧ ОКР «Амезит-В» СПО ПРР должно обеспечивать распространение информационных сообщений абонентам по телефонным сетям, используя технологию IP-телефонии.

А.93.3 Для проведения проверки СПО ПРР на соответствие предъявляемым требованиям необходимо выполнить действия, описанные ниже.

А.93.3.1 Запустить обозреватель.

А.93.3.2 Ввести в адресной строке обозревателя адрес веб-интерфейса СПО ПРР и пройти авторизацию в системе.

А.93.3.3 Перейти в раздел «Мероприятия».

А.93.3.4 Слева в списке «Объектов» выбрать коллекцию «Мероприятия ПИМ» (созданную в пункте А.82.3.5).

А.93.3.5 На панели команд нажать на кнопку «+ Мероприятие».

А.93.3.6 В открывшемся окне задать следующие параметры мероприятия:

- «Название»: ПИМ Телефонные вызовы;
- «Тип мероприятия»: Телефония;
- «Сценарий»: Телефонные вызовы;
- «SIM-карты»: выберите 3 произвольных SIM-карты из списка;
- «Начало»: задать текущее время;
- «Завершение»: задать время через 20 минут от текущего;
- «Абоненты»: указать номер мобильного телефона, используемого для тестирования;
- «Библиотека сообщений»: выбрать библиотеку «Тестовый звонок» (подготовленной и загруженной ранее);
- «Количество попыток»: установить значение 3;
- «Период между попытками»: установить значение 30.

А.93.3.7 Нажать на кнопку «Сохранить».

А.93.3.8 Дождаться завершения создания мероприятия.

А.93.3.9 Дождаться входящего вызова на телефон, используемый для проверки.

А.93.3.10 Принять входящий вызов и прослушать сообщение.

А.93.3.11 Перейти в раздел «Управление». В списке объектов выбрать «Параметры». Используя IP-адрес, логин и пароль, указанные в поле «Значение» параметра «Сервер IP-телефонии», подключиться к серверу и выполнить вход в веб-интерфейс.

А.93.3.12 Выбрать пункт меню «Отчеты» - «Логфайлы Asterisk». В поле «Filter» ввести «\[<номер мобильного телефона для тестирования в формате 79161234567>@from-internal». Нажать на кнопку «Show». Проверить наличие актуальных записей журнала о совершенном проверочном звонке.

А.93.3.13 Выбрать пункт меню «Отчеты» - «Call Event Logging». Нажать на кнопку «Поиск». Проверить наличие в списке совершенного проверочного звонка.

А.93.4 СПО ПРР считается выдержавшим испытания по п. А.93.3.1-А.93.3.10 программы и методики испытаний и выполняющим пункты 3.2.7, 3.2.7.14 ТЗ на СЧ ОКР, если:

- входящий телефонный вызов был осуществлен с одного из номеров, указанных в поле «SIM-карты» при создании мероприятия;
- прослушанное сообщение соответствовало сообщению, загруженному в библиотеку «Тестовый звонок»;
- на сервере IP-телефонии журнале и истории звонков присутствовали записи о совершенном проверочном звонке.

А.94 Методика № 94

А.94.1 В данной методике проводится проверка СПО ПРР на соответствие требованиям пунктов 3.2.7, 3.2.7.15 ТЗ на СЧ ОКР «Амезит-В».

А.94.2 В соответствии с требованиями пунктов 3.2.7, 3.2.7.15 ТЗ на СЧ ОКР «Амезит-В» СПО ПРР должно обеспечивать распространение информационных сообщений абонентам посредством SMS/MMS-сообщений.

А.94.3 Для проведения проверки СПО ПРР на соответствие предъявляемым требованиям необходимо выполнить действия, описанные ниже.

А.94.3.1 Запустить обозреватель.

А.94.3.2 Ввести в адресной строке обозревателя адрес веб-интерфейса СПО ПРР и пройти авторизацию в системе.

А.94.3.3 Перейти в раздел «Мероприятия».

А.94.3.4 Слева в списке «Объектов» выбрать коллекцию «Мероприятия ПИМ» (созданную в пункте А.82.3.5).

А.94.3.5 На панели команд нажать на кнопку «+ Мероприятие».

А.94.3.6 В открывшемся окне задать следующие параметры мероприятия:

- «Название»: ПИМ SMS-рассылка;
- «Тип мероприятия»: Телефония;
- «Сценарий»: Рассылка СМС-сообщений;
- «SIM-карты»: выбрать 3 произвольных SIM-карты из списка;
- «Начало»: задать текущее время;
- «Завершение»: задать время через 10 минут от текущего;
- «Номера получателей»: ввести номер мобильного телефона, используемого для тестирования;
- «Библиотека сообщений»: выбрать из библиотеки «ПИМ Сообщения СМС» (должна быть заранее подготовлена и наполнена в соответствии с документом RU.ВАТС.00183-01 92 01 «Специальное программное обеспечение подсистемы подготовки, размещения и «раскрутки» специальных материалов. Руководство пользователя»);
- «Количество СМС абоненту»: указать значение 3.

А.94.3.7 Нажать на кнопку «Сохранить».

А.94.3.8 Дождаться завершения выполнения мероприятия.

А.94.3.9 В процессе выполнения мероприятия на телефонный номер, указанный в пункте А.94.3.6, должно поступить 3 СМС-сообщения.

А.94.4 СПО ПРР считается выдержавшим испытания по п. А.94.3.1-А.94.3.9 программы и методики испытаний и выполняющим пункты 3.2.7, 3.2.7.15 ТЗ на СЧ ОКР, если:

- полученные СМС-сообщения отправлены с номеров, указанных в поле «SIM-карты» (любых из них);
- содержимое сообщений соответствует сообщениям, входящим в библиотеку «ПИМ Сообщения СМС».

А.95 Методика № 95

А.95.1 В данной методике проводится проверка СПО ПРР на соответствие требованиям пунктов 3.2.7, 3.2.7.16 ТЗ на СЧ ОКР «Амезит-В».

А.95.2 В соответствии с требованиями пунктов 3.2.7, 3.2.7.16 ТЗ на СЧ ОКР «Амезит-В» СПО ПРР должно обеспечивать информационное обеспечение мероприятий по распространению специальных материалов в поддерживаемых сервисах должно обеспечиваться следующими функциями:

- анализ заданных оператором текстовых материалов и генерация релевантных им ключевых слов (хештегов);
- анализ эффективности распространения информационных материалов, включающий динамику публикаций и активность отклика со стороны пользователей социальных сетей.

Примечание. Информационное обеспечение мероприятий по распространению материалов должно осуществляться с учетом «Методики повышения эффективности распространения специальных и контрпропагандистских материалов», согласованной с головным исполнителем (см. п. 13.3.9 ТЗ).

А.95.3 Для проведения проверки СПО ПРР на соответствие предъявляемым требованиям необходимо выполнить действия, описанные ниже.

А.95.3.1 Запустить обозреватель.

А.95.3.2 Ввести в адресной строке обозревателя адрес веб-интерфейса СПО ПРР и пройти авторизацию в системе.

А.95.3.3 Проверка анализа заданных оператором текстовых материалов и генерация релевантных им ключевых слов выполняется в следующем порядке:

А.95.3.3.1 Перейти в раздел «Библиотеки».

А.95.3.3.2 В списке «Объектов» нажать на «Сообщения».

А.95.3.3.3 На панели команд нажать на кнопку «+Библиотека».

А.95.3.3.4 Ввести название библиотеки «ПИМ анализ».

А.95.3.3.5 Добавить в библиотеку произвольный текст длиной не менее 1000 символов. Для получения текста выполнить следующие действия:

- в обозревателе перейти по адресу https://news.google.ru;
- ыыбрать произвольную новость с достаточным количеством символов (не менее 1000).

А.95.3.3.6 Скопировать текст новости в буфер обмена и вставить его в поле «Текст» создаваемого сообщения библиотеки.

А.95.3.3.7 Нажать на кнопку «Сохранить».

А.95.3.3.8 Навести курсор на заголовок созданного сообщения.

А.95.3.3.9 Нажать в заголовке сообщения на отобразившейся кнопке «#».

А.95.3.3.10 В открывшемся модальном окне «Рекомендация хештегов» ввести: «Количество хештегов»: 10.

А.95.3.3.11 Нажать на кнопку «Анализ» в открытом диалоговом окне.

А.95.3.3.12 Дождаться завершения анализа.

А.95.3.3.13 Убедиться, что в модальном окне отобразилось от 1 до 10 предложенных хештегов.

А.95.3.3.14 Нажать на кнопку «Сохранить».

А.95.3.3.15 Навести курсор на заголовок сообщения, для которого производился анализ, и нажать на отобразившуюся кнопку редактирования.

А.95.3.3.16 Убедиться в отобразившемся модальном окне, что в поле «Хештеги» присутствуют рекомендованные хештеги.

А.95.3.4 Проверка анализа эффективности распространения информационных материалов, включающая динамику публикаций и активность отклика со стороны пользователей социальных сетей, выполняется в следующем порядке:

А.95.3.4.1 Перейти в раздел «Мероприятия».

А.95.3.4.2 Открыть коллекцию мероприятий «Мероприятия ПИМ».

А.95.3.4.3 Открыть мероприятие «ПИМ Размещение материалов» (созданное при выполнении методики № Методика № 91) или любое другое с типом «Размещение публикаций».

А.95.3.4.4 В панели команд нажать на кнопку «Отчет».

А.95.3.4.5 В открывшемся диалоговом окне выбрать следующие разделы отчета:

- «динамика публикаций»: включено;
- «интервал расчета»: 10 минут;
- «отклик пользователей»: включено.

А.95.3.4.6 Нажать на кнопку «Создать».

А.95.3.4.7 Дождаться завершения формирования отчета.

А.95.3.4.8 Нажать на кнопку «Сохранить».

А.95.3.4.9 Открыть файл в Microsoft Office Word.

А.95.4 СПО ПРР считается выдержавшим испытания по п. А.95.3.1-А.95.3.4.9 программы и методики испытаний и выполняющим пункты 3.2.7, 3.2.7.16 ТЗ на СЧ ОКР, если проверка в пункте А.95.3.3.7 выполнена успешно и содержимое файла отчета по мероприятию (пункт А.95.3.4.9) содержит следующие данные:

- время проведения мероприятия по распространению материалов;
- название мероприятия;
- таблицу с интервалами времени с шагом в 10 мин, содержащую информацию о количестве размещенных публикаций в данный интервал времени, количестве полученных одобрений, перепечаток и комментариев к данным публикациям.

A.96 Методика № 96

A.96.1 В данной методике проводится проверка СПО ПРР на соответствие требованиям пункта 3.2.7.17 ТЗ на СЧ ОКР «Амезит-В».

A.96.2 В соответствии с требованиями пунктов 3.2.7, 3.2.7.17 ТЗ на СЧ ОКР «Амезит-В» в процессе распространения информационных материалов подсистема ПРР должна обеспечивать «эффект реального пользователя» следующими способами:

- автоматическое ведение жизнедеятельности виртуальных пользователей, включающее следующие действия: наполнение личных страниц публикациями в соответствии с их личными интересами, добавление друзей, вступление в группы, просмотр страниц социальных сетей в режиме чтения («серфинг»);
- при работе с социальными сетями должны имитироваться действия реальных пользователей;
- посимвольный ввод данных, переходы по ссылкам, прокрутка страниц, задержки между действиями.

A.96.3 Для проведения проверки СПО ПРР на соответствие предъявляемым требованиям необходимо выполнить действия, описанные ниже.

A.96.3.1 Выполнить подготовку ВМ агентов для данной проверки:

A.96.3.1.1 Используя обозреватель и документ RU.ВАТС.00183-01 32 01 «Специальное программное обеспечение подсистемы подготовки, размещения и «раскрутки» специальных материалов. Руководство системного программиста», подключиться к любому из серверов виртуализации.

A.96.3.1.2 Ввести логин и пароль входа в среду виртуализации «Proxmox VE».

A.96.3.1.3 Выключить все ВМ агентов.

A.96.3.1.4 Запустить только одну ВМ агентов.

A.96.3.1.5 Открыть запущенную ВМ агентов.

A.96.3.1.6 Перейти в раздел «Консоль» и авторизоваться в системе с использованием логина и пароля пользователя на данной ВМ.

A.96.3.1.7 Отредактировать файл /etc/prr/agent.conf, изменив в нем параметр «headless: yes» на «headless: no».

A.96.3.1.8 Выполнить команду в консоли: sudo god agents restart.

A.96.3.2 Открыть новое окно обозревателя.

A.96.3.3 Ввести в адресной строке обозревателя адрес веб-интерфейса СПО ПРР и пройти авторизацию в системе.

А.96.3.4 Перейти в раздел «Журналы».

А.96.3.5 Проверить наличие записей об успешных действиях следующих типов:

- «Публикация»;
- «Подписка на пользователя»;
- «Перепубликация».

А.96.3.6 Перейти на страницу любого пользователя, выполнившего успешные действия «Публикация». Проверить наличие на странице пользователя размещенной публикации, выполненной в рамках автоматической жизнеятельности.

А.96.3.7 Перейти в раздел «Мероприятия».

А.96.3.8 В меню «Объектов» выбрать коллекцию «Мероприятия ПИМ».

А.96.3.9 Перезапустить мероприятие «ПИМ Подписка на пользователя», изменив время проведения мероприятия на текущее и нажав на кнопку «Перезапустить» в строке мероприятия.

А.96.3.10 Переключиться на окно обозревателя с окном виртуальной машины, открытого ранее (п. А.96.3.1).

А.96.4 СПО ПРР считается выдержавшим испытания по п. А.96.3.1-А.96.3.10 программы и методики испытаний и выполняющим пункт 3.2.7.17 ТЗ на СЧ ОКР, если в процессе проведения перезапущенного мероприятия (пункт А.96.3.9) на экране ВМ агентов:

- запускаются окна обозревателей виртуальных пользователей;
- виртуальные пользователи выполняют процедуру входа в социальную сеть;
- виртуальные пользователи выполняют действия подписки на пользователя, имитируя работу с обозревателем;
- виртуальные пользователи выполняют размещение публикаций в рамках автоматической жизнедеятельности.

П р и м е ч а н и е. После завершения методики запускают все виртуальные машины агентов в интерфейсе «Proxmox VE».

А.97 Методика № 97

А.97.1 В данной методике проводится проверка СПО ПРР на соответствие требованиям пункта 3.2.7.18 ТЗ на СЧ ОКР «Амезит-В».

А.97.2 В соответствии с требованиями пунктов 3.2.7, 3.2.7.18 ТЗ на СЧ ОКР «Амезит-В» действия СПО технических средств «раскрутки» материалов не должны раскрывать национальную и ведомственную принадлежность. Для этого должны быть реализованы следующие механизмы:

- управление действиями виртуальных пользователей посредством графического интерфейса подсистемы: отправка личных сообщений, добавление в друзья, вступление в группы, размещение публикаций, отправка комментариев. Выполнение данных действий виртуальным пользователем должно происходить в соответствии с индивидуальным графиком активности либо в заданный оператором момент времени;

- взаимодействие с поддерживаемыми сервисами должно происходить только через подсистему ПРД;

- предоставление оператору всех необходимых данных для работы из-под конкретной учетной записи: логин и пароль, требуемые настройки обозревателя и окружения.

Примечания:

1. Должна быть реализована функция проверки прикладного программного обеспечения, исходя из легенды виртуального пользователя (поддерживаемые обозревателем раскладки клавиатуры, версию и язык операционной системы и т.д.).

2. Должна быть реализована функция блокирования использования подсистемы ПРР в личных целях.

3. Должна быть реализована возможность многопользовательского использования СПО подсистемы ПРР территориально распределенными элементами АПК «Амезит» (через подсистему ППД).

А.97.3 Для проведения проверки СПО ПРР на соответствие предъявляемым требованиям необходимо выполнить действия, описанные ниже.

А.97.3.1 Проверка выполнения действий (отправка личных сообщений, добавление в друзья, вступление в группы, размещение публикаций, отправка комментариев) виртуальным пользователем в соответствии с индивидуальным графиком активности либо в заданный оператором момент времени проводится в следующем порядке:

А.97.3.1.1 Запустить обозреватель.

А.97.3.1.2 Ввести в адресной строке обозревателя адрес веб-интерфейса СПО ПРР и пройти авторизацию в системе.

А.97.3.1.3 Перейти в раздел «Пользователи».

А.97.3.1.4 В левом меню объектов нажать на кнопку фильтрации пользователей.

А.97.3.1.5 В фильтрах выбрать:

- в выпадающем списке выбрать «Все сообщества»;

- сервисы «ВКонтакте».

А.97.3.1.6 В рабочей области в столбце «Пользователь» нажать на ссылку левой кнопкой мыши.

А.97.3.1.7 В панели команд нажать на кнопку кнопку «+Задача».

А.97.3.1.8 В поле «Аккаунт» выбрать аккаунт сервиса «ВКонтакте».

А.97.3.1.9 Проверить содержимое списка доступных задач в поле «Тип задачи».

А.97.3.1.10 Выбрать в поле «Тип задачи» значение «Публикация».

А.97.3.1.11 В параметрах задачи задать значения:

- в поле «Начало задачи»: время через 5 минут от текущего;
- в поле «Текст»: Мой новый пост;
- в поле «Ссылки»: http://ya.ru;
- в поле «Хештеги»: тег публикации.

А.97.3.1.12 Нажать на кнопку «Сохранить».

А.97.3.1.13 В панели команд нажать на кнопку «Задачи».

А.97.3.1.14 В правом верхнем углу рабочей области выбрать значение фильтра «Планируемые».

А.97.3.1.15 Найти в списке планируемых задач созданную задачу на публикацию.

А.97.3.1.16 Нажать на кнопку «Просмотр» для данной задачи.

А.97.3.1.17 Проверить параметры задачи на соответствие заданным.

А.97.3.1.18 Удалить задачу из списка запланированных задач, нажав на значок удаления в строке с задачей.

А.97.3.1.19 Убедиться, что удаленная задача отсутствует в списке запланированных.

А.97.3.2 Проверка взаимодействия с поддерживаемыми сервисами только через СПО ПРД проводится в следующем порядке:

А.97.3.2.1 Заблокировать доступ к ресурсам ГИС Интернет для пользователей СПО ПРР.

А.97.3.2.2 Выполнить мероприятие «ПИМ Вступление в группу» согласно методике Методика № 82.

А.97.3.2.3 Убедиться, что результат повторного испытания отрицательный (виртуальными пользователями не должно быть выполнено успешно ни одного действия).

А.97.3.3 Проверка предоставления оператору данных для работы из-под конкретной учетной записи виртуального пользователя проводится в следующем порядке:

А.97.3.3.1 Ввести в адресной строке обозревателя адрес веб-интерфейса СПО ПРР и пройти авторизацию в системе.

А.97.3.3.2 Перейти в раздел «Пользователи».

А.97.3.3.3 Выбрать случайного виртуального пользователя нажатием левой кнопкой мыши на ссылке в столбце «Пользователь» в рабочей области.

А.97.3.3.4 Убедиться, что для каждого доступного аккаунта у пользователя отображаются его сервис, логин и пароль.

А.97.3.3.5 На панели команд нажать на кнопку «Сессия».

А.97.3.3.6 Проверить данные сессии пользователя для доступа.

А.97.3.4 Проверку блокирования использования подсистемы ПРР в личных целях выполняют в следующем порядке:

А.97.3.4.1 Выполнить мероприятие «ПИМ Вступление в группу» согласно методике Методика № 82 для пользователя с ролью «Оператор».

А.97.3.4.2 Убедиться, что созданное мероприятие не начинает выполняться. Состояние мероприятия в списке мероприятий должно отображаться как «Ожидает подтверждения».

А.97.3.4.3 Войти в СПО ПРР от имени пользователя с ролью «Пользователь».

А.97.3.4.4 Перейти в раздел «Мероприятия».

А.97.3.4.5 Выбрать коллекцию, в которой было создано мероприятие «ПИМ Вступление в группу».

А.97.3.4.6 Убедиться, что созданное мероприятие отображается с состоянием «Ожидает подтверждения», рядом с состоянием отображается кнопка «Подтвердить».

А.97.3.4.7 Нажать на кнопку «Подтвердить» для данного мероприятия.

А.97.3.4.8 Проверить изменение состояния мероприятия.

А.97.3.4.9 СПО ПРР считается выдержавшим испытания по п. А.97.3.1-А.97.3.4.9 программы и методики испытаний и выполняющим пункт 3.2.7.18 ТЗ на СЧ ОКР, если:

- список доступных задач виртуального пользователя содержит:
  - личное сообщение;
  - подписка на пользователя;
  - вступление в группу;
  - публикация;
  - комментарий;
  - одобрение;
  - перепечатка.
- параметры задач пользователя соответствуют заданным;

- удаленная задача пользователя отсутствует в списке запланированных;
- при блокировке ресурсов с помощью СПО ПРД созданное мероприятие не выполняется;
- для каждого доступного аккаунта виртуального пользователя отображаются его сервис, логин и пароль;
- в данных сессии пользователя присутствуют следующие записи:
  - user-agent браузера;
  - прокси-сервер;
  - разрешение экрана пользователя;
  - временная зона пользователя;
  - язык пользователя;
  - команда для запуска браузера «Chromium».
- пользователь с ролью «Оператор» не может запустить созданное мероприятие на выполнение; подтверждение мероприятия пользователем с ролью «Пользователь» переводит мероприятие в состояние «Запущена».

А.98 Методика № 98

А.98.1 В данной методике проводится проверка СПО ПРР на соответствие требованиям п. 3.2.7.19 ТЗ на СЧ ОКР «Амезит-В».

А.98.2 В соответствии с требованиями пунктов п. 3.2.7.19 ТЗ на СЧ ОКР «Амезит-В» СПО ПРР должно обеспечивать автоматизированное взаимодействие с СПО подсистемы лингвистического обеспечения.

А.98.3 Для проведения проверки СПО ПРР на соответствие предъявляемым требованиям необходимо выполнить действия, описанные ниже.

А.98.3.1 Настроить путь к серверу подсистемы лингвистического обеспечения, задав значение plo_server в файле конфигурации config/config.yml (действие выполняет администатор АПК «Амезит»).

А.98.3.2 Запустить обозреватель.

А.98.3.3 В адресной строке обозревателя ввести адрес веб-интерфейса СПО ПРР и проходят авторизацию в системе.

А.98.3.4 Перейти в раздел «Библиотеки».

А.98.3.5 Слева в меню объектов выбрать подраздел «Сообщения».

А.98.3.6 Слева в списке «Библиотеки сообщений» выбрать любую непустую библиотеку сообщений.

А.98.3.7 В рабочей области навести курсор на заголовок любого сообщения.

А.98.3.8	В заголовке сообщения нажать на отобразившуюся кнопку «» («Перевести»).

А.98.3.9	В открывшемся модальном окне «Перевод сообщения» в поле «Текст» ввести текст для перевода «hello test one two three».

А.98.3.10	Нажать на кнопку «Выполнить».

А.98.3.11	Дождаться получения результата перевода в поле «Перевод».

А.98.3.12	Для просмотра формата передаваемых данных в обозревателе открыть консоль разработчика (комбинацией клавиш Ctrl+J) и перейти на вкладку «Network» («Сеть»).

А.98.4	СПО ПРР считается выдержавшим испытания по п. А.98.3.1-А.98.3.12 программы и методики испытаний и выполняющим пункт 3.2.7.18 ТЗ на СЧ ОКР, если:

- при выполнении вышеуказанных действий данной методики отсутствовали сообщения об ошибках;
- при выполнении перевода текста сообщения получен текст «привет проверка один два три»;
- при просмотре формата передаваемых данных форматы отправленных и полученных данных соответствуют принятым форматам ПЛО.

А.99	Методика № 99

А.99.1	В данной методике проводится проверка СПО ПРР на соответствие требованиям пунктов 9.3.2, 9.3.3 ТЗ на СЧ ОКР «Амезит-В».

А.99.2	В соответствии с требованиями пунктов 9.3.2, 9.3.3 ТЗ на СЧ ОКР «Амезит-В» СПО ПРР должно обеспечивать выполнение требований по режиму обработки данных и правам по доступу к обрабатываемой информации.

А.99.3	Для проведения проверки СПО ПРР на соответствие предъявляемым требованиям необходимо выполнить действия, описанные ниже.

А.99.3.1	Запустить обозреватель.

А.99.3.2	Ввести в адресной строке обозревателя адрес веб-интерфейса СПО ПРР.

А.99.3.3	В открывшемся окне авторизации ввести заведомо неверные логин и/или пароль (логин – AnyUser, пароль – somePassword).

А.99.3.4	После нажатия на кнопку «Войти» должно отобразиться сообщение об ошибке несанкционированного доступа и в отсутствии доступа к СПО.

А.99.3.5	Пройти авторизацию в системе с действительными данными в соответствии с документом RU.ВАТС.00183-01 92 01 «Специальное

программное обеспечение подсистемы подготовки, размещения и «раскрутки» специальных материалов. Руководство пользователя».

А.99.3.6 После нажатия на кнопку «Войти» должен открыться основной интерфейс СПО ПРР, что свидетельствует об успешном получении доступа к СПО.

А.99.4 СПО ПРР считается выдержавшим испытания по п. А.99.3.1-А.99.3.6 программы и методики испытаний и выполняющим пункты 9.3.2, 9.3.3 ТЗ на СЧ ОКР, если в пункте А.99.3.4 доступ пользователю не предоставлен и выведено сообщение об ошибке, а в пункте А.99.3.6 пользователь успешно вошел в систему.

А.100 Методика № 100

А.100.1 В данной методике проводится проверка СПО ПРР на соответствие требованиям пункта 9.17 ТЗ на СЧ ОКР «Амезит-В».

А.100.2 В соответствии с требованиями п. 9.17 ТЗ на СЧ ОКР «Амезит-В» СПО ПРР должно обеспечивать выполнение функций регистрации и хранения действий операторов.

А.100.3 Для проведения проверки СПО ПРР на соответствие предъявляемым требованиям необходимо выполнить действия, описанные ниже.

А.100.3.1 В соответствии с документом RU.ВАТС.00183-01 32 01 «Специальное программное обеспечение подсистемы подготовки, размещения и «раскрутки» специальных материалов. Руководство системного программиста» подключиться к серверу интерфейса управления через SHH-клиент от имени суперпользователя. Доменное имя для подключения (Hostname): ui.srv.

А.100.3.2 В окне SSH-клиента ввести команду: tail –f /srv/ prr-ui/logs/*log.

А.100.3.3 Запустить обозреватель и в адресной строке ввести адрес интерфейса управления СПО ПРР.

А.100.4 СПО ПРР считается выдержавшим испытания по п. А.100.3.1-А.100.3.3 программы и методики испытаний и выполняющим пункт 9.17 ТЗ на СЧ ОКР, если после выполнения пункта А.100.3.3 в окне SSH-клиента будут отображены данные запроса к интерфейсу управления следующего вида:

```
Started GET "<путь запроса>" for <IP-клиента> at <Время запроса>
Processing by <Контролер и метод обработки запроса через #>
```

Например:

```
Started GET "/" for 10.10.10.10 at 2018-04-20 13:15:42
Processing by AuthController#login
```

A.101 Методика № 101

А.101.1 В данной методике проводится проверка СПО ПТТ на соответствие требованиям пунктов 3.2.8, 3.2.8.1 ТЗ на СЧ ОКР «Амезит-В».

А.101.2 В соответствии с требованиями пунктов 3.2.8, 3.2.8.1 ТЗ на СЧ ОКР «Амезит-В» СПО ПТТ должно обеспечивать обнаружение актуальных критических уязвимостей ОС Microsoft Windows XP и старше, Microsoft Windows Server 2003 и старше, Red Hat 5 и старше, CentOS 5 и старше, Debian 6 и старше, Ubuntu 12 и старше. Актуальность версий ПО устанавливается на дату утверждения программы и методик предварительных испытаний.

А.101.3 Для проведения проверки СПО ПТТ на соответствие предъявляемым требованиям необходимо выполнить действия, описанные ниже.

А.101.3.1 Убедиться в наличии комплекта программно-технических средств, включающего ПЭВМ с установленными ОС Microsoft Windows XP и старше, Microsoft Windows Server 2003 и старше, Red Hat 5 и старше, CentOS 5 и старше, Debian 6 и старше, Ubuntu 12 и старше.

Примечание. Допускается использование ВМ, имитирующих ПЭВМ, работающих под управлением перечисленных ОС.

А.101.3.2 Выбрать одну из ПЭВМ, перечисленных в пункте А.101.3.1, и выполнить сканирование программных компонентов ОС данной ПЭВМ с помощью сканера уязвимостей MaxPatrol. Проверка выполняется в соответствии с документом RU.BATC.00184-01 92 02 «Специальное программное обеспечение подсистемы тестирования телекоммуникационного оборудования. ПО MaxPatrol. Руководство пользователя».

А.101.3.3 Выполнить операции по статическому и структурному анализу кода в соответствии с пунктом А.104 для компонентов ОС, к которым имеются исходные тексты программ.

Примечание. Допускается совмещение данного действия с проверкой, выполняемой в пункте А.104 (методика Методика № 104).

А.101.3.4 Выполнить операции по динамическому анализу кода ОС в соответствии с пунктом А.105.

Примечание. Допускается совмещение данного действия с проверкой, выполняемой в пункте А.105 (методика Методика № 105).

А.101.3.5 Выполнить операции по автоматизированному распознаванию стандартных библиотечных функций, используемых в ОС, в соответствии с пунктом А.106.

Примечание. Допускается совмещение данного действия с проверкой, выполняемой в пункте А.106 (методика Методика № 106).

А.101.3.6 Выполнить операции по сигнатурному анализу опасных операций, выполняемых в ОС, в соответствии с пунктом А.107.

Примечание. Допускается совмещение данного действия с проверкой, выполняемой в пункте А.107 (методика Методика № 107).

А.101.3.7 Выполнить операции по автоматизированному поиску внесенных изменений в программный код ОС при его модификации в соответствии с пунктом А.111.

Примечание. Допускается совмещение данного действия с проверкой, выполняемой в пункте А.111 (методика Методика № 111).

А.101.4 СПО ПТТ считается выдержавшим испытания по п. А.101.3.1-А.101.3.7 программы и методики испытаний и выполняющим пункты 3.2.8, 3.2.8.1 ТЗ на СЧ ОКР, если:

- по результатам проверок, выполненных в пунктах А.101.3.2–А.101.3.7, получены отчеты, содержащие корректные и непротиворечивые данные об уязвимостях проверенных ОС;
- ПО, используемое при проведении проверок, осуществляет поиск и обнаружение уязвимостей проверяемых ОС.

А.102 Методика № 102

А.102.1 В данной методике проводится проверка СПО ПТТ на соответствие требованиям пунктов 3.2.8, 3.2.8.2 ТЗ на СЧ ОКР «Амезит-В».

А.102.2 В соответствии с требованиями пунктов 3.2.8, 3.2.8.2 ТЗ на СЧ ОКР «Амезит-В» СПО ПТТ должно обеспечивать обнаружение актуальных критических уязвимостей MS SQL Server 2008/2008R2/2012, Oracle Database 10 for Linux/Windows, Oracle MySQL 4.x. и Microsoft Office 2003 и выше, Adobe, OpenOffice для Linux-платформ, браузерах Microsoft Explorer, Opera, FireFox, Google Chrome, ПО Adobe Reader, Adobe Flash. Актуальность версий ПО устанавливается на дату утверждения программы и методик предварительных испытаний.

А.102.3 Для проведения проверки СПО ПТТ на соответствие предъявляемым требованиям необходимо выполнить действия, описанные ниже.

А.102.3.1 Убедиться в наличии комплекта программно-технических средств, включающего ПЭВМ с установленным ПО MS SQL Server 2008/2008R2/2012, Oracle Database 10 for Linux/Windows, Oracle MySQL 4.x. и Microsoft Office 2003 и выше, Adobe, OpenOffice для Linux-платформ, браузерами Microsoft Explorer, Opera, FireFox, Google Chrome, ПО Adobe Reader, Adobe Flash.

Примечание. Допускается использование ВМ, имитирующих ПЭВМ с установленным на них перечисленным ПО.

А.102.3.2 Выбрать одну из ПЭВМ с установленным ПО, перечисленным в пункте А.102.3.1. Выбрать одну программу из ПО, установленного на ПЭВМ, и выполнить ее сканирование с помощью сканера уязвимостей MaxPatrol. Проверка выполняется в соответствии с документом RU.BATC.00184-01 92 02 «Специальное программное обеспечение подсистемы тестирования телекоммуникационного оборудования. ПО MaxPatrol. Руководство пользователя».

А.102.3.3 Выполнить операции по статическому и структурному анализу кода в соответствии с пунктом А.104 для компонентов ПО, к которым имеются исходные тексты программ.

Примечание. Допускается совмещение данного действия с проверкой, выполняемой в пункте А.104 (методика Методика № 104).

А.102.3.4 Выполнить операции по динамическому анализу кода ПО в соответствии с пунктом А.105.

Примечание. Допускается совмещение данного действия с проверкой, выполняемой в пункте А.105 (методика Методика № 105).

А.102.3.5 Выполнить операции по автоматизированному распознаванию стандартных библиотечных функций, используемых в ПО, в соответствии с пунктом А.106.

Примечание. Допускается совмещение данного действия с проверкой, выполняемой в пункте А.106 (методика Методика № 106).

А.102.3.6 Выполнить операции по сигнатурному анализу опасных операций, выполняемых ПО, в соответствии с пунктом А.107.

Примечание. Допускается совмещение данного действия с проверкой, выполняемой в пункте А.107 (методика Методика № 107).

А.102.3.7 Выполнить операции по автоматизированному поиску внесенных изменений в программный код ПО при его модификации в соответствии с пунктом А.111.

Примечание. Допускается совмещение данного действия с проверкой, выполняемой в пункте А.111 (методика Методика № 111).

А.102.4 СПО ПТТ считается выдержавшим испытания по п. А.102.3.1-А.102.3.7 программы и методики испытаний и выполняющим пункты 3.2.8, 3.2.8.2 ТЗ на СЧ ОКР, если:

- по результатам проверок, выполненных в пунктах А.102.3.2–А.102.3.7, получены отчеты, содержащие корректные и непротиворечивые данные об уязвимостях проверенного ПО;

- ПО, используемое при проведении проверок, осуществляет поиск и обнаружение уязвимостей проверяемых программ.

А.103 Методика № 103

А.103.1 В данной методике проводится проверка СПО ПТТ на соответствие требованиям пунктов 3.2.8, 3.2.8.4 ТЗ на СЧ ОКР «Амезит-В».

А.103.2 В соответствии с требованиями пунктов 3.2.8, 3.2.8.4 ТЗ на СЧ ОКР «Амезит-В» СПО ПТТ должно обеспечивать обнаружение актуальных критических уязвимостей ПО защиты информации, в составе которого присутствует системное, серверное и прикладное ПО, перечисленное в пп. А.101.2, А.102.2 настоящего документа.

А.103.3 Для проведения проверки СПО ПТТ на соответствие предъявляемым требованиям необходимо выполнить действия, описанные ниже.

А.103.3.1 Убедиться в наличии комплекта программно-технических средств, включающего ПЭВМ с установленными на них тремя различными экземплярами ПО средств защиты информации, в составе которых присутствует системное, серверное и прикладное ПО, перечисленное в пунктах 3.2.8.1, 3.2.8.2 ТЗ на СЧ ОКР «Амезит-В».

Примечание. Допускается использование ВМ, имитирующих ПЭВМ с установленным на них ПО средств защиты информации.

А.103.3.2 Выбрать одну из ПЭВМ с установленным ПО, перечисленным в пункте А.103.3.1. Выбрать одну программу средств защиты информации, установленную на выбранную ПЭВМ, и выполнить ее сканирование с помощью сканера уязвимостей MaxPatrol. Проверка выполняется в соответствии с документом RU.ВАТС.00184-01 92 02 «Специальное программное обеспечение подсистемы тестирования телекоммуникационного оборудования. ПО MaxPatrol. Руководство пользователя».

А.103.3.3 Выполнить операции по статическому и структурному анализу кода в соответствии с пунктом А.104 для компонентов ПО средств защиты информации, к которым имеются исходные тексты программ.

Примечание. Допускается совмещение данного действия с проверкой, выполняемой в пункте А.104 (методика Методика № 104).

А.103.3.4 Выполнить операции по динамическому анализу кода ПО средств защиты информации в соответствии с пунктом А.105.

Примечание. Допускается совмещение данного действия с проверкой, выполняемой в пункте А.105 (методика Методика № 105).

А.103.3.5 Выполнить операции по автоматизированному распознаванию стандартных библиотечных функций, используемых в ПО средств защиты информации, в соответствии с пунктом А.106.

Примечание. Допускается совмещение данного действия с проверкой, выполняемой в пункте А.106 (методика Методика № 106).

А.103.3.6 Выполнить операции по сигнатурному анализу опасных операций, выполняемых ПО средств защиты информации, в соответствии с пунктом А.107.

Примечание. Допускается совмещение данного действия с проверкой, выполняемой в пункте А.107 (методика Методика № 107).

А.103.3.7 Выполнить операции по автоматизированному поиску внесенных изменений в программный код ПО средств защиты информации при его модификации в соответствии с пунктом А.111.

Примечание. Допускается совмещение данного действия с проверкой, выполняемой в пункте А.111 (методика Методика № 111).

А.103.3.8 Проверка возможности обнаружения актуальных критических уязвимостей ПО средств защиты информации считается пройденной успешно, если:

- по результатам проверок, выполненных в пунктах А.103.3.2–А.103.3.7, получены отчеты, содержащие корректные и непротиворечивые данные об уязвимостях проверенного ПО средств защиты информации;
- ПО, используемое при проведении проверок, осуществляет поиск и обнаружение уязвимостей проверяемых программ средств защиты информации.

А.103.3.9 Проверка наличия в составе СПО ПТТ ПО Immunity CANVAS выполняется в соответствии с пунктами А.103.3.10, А.103.3.11.

А.103.3.10 Для проверки необходимо запустить ПО Immunity CANVAS и продемонстрировать его работоспособность на примере выбранного образца ПО.

А.103.3.11 Проверка наличия в составе СПО ПТТ ПО Immunity CANVAS считается выполненной успешно, если в состав СПО ПТТ включено работоспособное ПО Immunity CANVAS.

А.103.4 СПО ПТТ считается выдержавшим испытания по п. А.103.3.1-А.103.3.11 программы и методики испытаний и выполняющим пункты 3.2.8, 3.2.8.4 ТЗ на СЧ ОКР, если выполнены условия в пунктах А.103.3.8 и А.103.3.11.

А.104 Методика № 104

А.104.1 В данной методике проводится проверка СПО ПТТ на соответствие требованиям пунктов 3.2.8, 3.2.8.5 ТЗ на СЧ ОКР «Амезит-В».

А.104.2 В соответствии с требованиями пунктов 3.2.8, 3.2.8.5 ТЗ на СЧ ОКР «Амезит-В» СПО ПТТ должно обеспечивать структурный и статический анализ исходных текстов программ на языках программирования:

- C;
- C++;
- NET;
- Java;
- PHP.

А.104.3 Для проведения проверки СПО ПТТ на соответствие предъявляемым требованиям необходимо выполнить действия, описанные ниже.

А.104.3.1 Проверка выполняется с использованием заранее подготовленных образцов ПО, представляющих собой файлы, разработанные на языках программирования C, C++, .NET, Java, PHP. В качестве образцов исходных текстов программ могут выступать файлы СПО АПК «Амезит», файлы любого свободно распространяемого ПО либо специально сформированные контрольные примеры.

А.104.3.2 Проверка выполняется в соответствии с документами RU.ВАТС.00184-01 92 08 «Специальное программное обеспечение подсистемы тестирования телекоммуникационного оборудования. ПО Application Inspector. Руководство пользователя», RU.ВАТС.00184-01 34 09 «Специальное программное обеспечение подсистемы тестирования телекоммуникационного оборудования. ПО PVS-Studio. Руководство пользователя».

А.104.3.3 Проверка статического (структурного) анализа контрольных образцов, в зависимости от языка программирования, выполняется с использованием соответствующего ПО (программного средства анализа), представленного в таблице .

Таблица 2 – Соответствие ПО статического (структурного) анализа проверяемым контрольным примерам

№ п/п	Наименование ПО статического (структурного) анализа (программное средство анализа)	Язык программирования проверяемых исходных текстов программ
1	PVS-Studio	C, C++
2	FindBugs	Java
3	BugScout	Java, .NET, C#, PHP
4	PT Application Inspector	Java, .NET, PHP

А.104.3.4 Для проведения проверки необходимо выполнить следующие действия:

А.104.3.4.1 Выбрать образец ПО, разработанный на одном из языков программирования, перечисленных в пункте А.104.2.

А.104.3.4.2 Выбрать программное средство анализа – ПО, соответствующее языку программирования, на котором разработан образец ПО.

А.104.3.4.3 Выполнить структурный и статический анализ образца ПО с использованием соответствующего программного средства анализа.

А.104.3.4.4 Убедиться в возможности проведения структурного и статического анализа образца ПО соответствующим программным средством анализа.

А.104.3.4.5 При необходимости дополнительно (по решению комиссии) выполнить пункты А.104.3.4.1–А.104.3.4.4 для любого другого произвольного образца ПО (нескольких произвольных образцов ПО).

А.104.4 СПО ПТТ считается выдержавшим испытания по п. А.104.3.4.1-А.104.3.4.5 программы и методики испытаний и выполняющим пункты 3.2.8, 3.2.8.5 ТЗ на СЧ ОКР, если программные средства анализа, перечисленные в таблице , обеспечивают проведение статического (структурного) анализа образцов ПО, разработанных на языках программирования, указанных в пункте А.104.2.

А.105 Методика № 105

А.105.1 В данной методике проводится проверка СПО ПТТ на соответствие требованиям пунктов 3.2.8, 3.2.8.6 ТЗ на СЧ ОКР «Амезит-В».

А.105.2 В соответствии с требованиями пунктов 3.2.8, 3.2.8.6 ТЗ на СЧ ОКР «Амезит-В» СПО ПТТ должно обеспечивать динамический анализ программного обеспечения.

А.105.3 Для проведения проверки СПО ПТТ на соответствие предъявляемым требованиям необходимо выполнить действия, описанные ниже.

А.105.3.1 Проверка обеспечения динамического анализа ПО выполняется с использованием заранее подготовленных файлов образцов ПО, представляющих собой скомпилированные бинарные модули. В качестве образцов бинарных модулей могут выступать исполняемые файлы и библиотеки СПО АПК «Амезит», исполняемые файлы и библиотеки любого ПО либо специально сформированные контрольные примеры.

А.105.3.2 Проверка файлов образцов ПО выполняется с использованием следующих программных средств анализа:

- дизассемблер – IDA Pro Disassembler;
- декомпилятор – Hex-Rays Decompiler;
- программа для фаззинга приложений – Peach Fuzzer;
- консольная утилита для фаззинга приложений – AFL;
- дополнительный модуль к ПО IDA Pro – ida-x86emu;
- отладчик – x64dbg.

А.105.3.3 Проверка выполняется в соответствии с документами RU.ВАТС.00184-01 92 10 «Специальное программное обеспечение подсистемы тестирования телекоммуникационного оборудования. ПО IDA Pro. Руководство пользователя», RU.ВАТС.00184-01 92 11 «Специальное программное обеспечение подсистемы тестирования телекоммуникационного оборудования. ПО x64dbg. Руководство пользователя».

А.105.3.4 Для проведения проверки необходимо выполнить следующие действия:

А.105.3.4.1 Выбрать образец ПО.

А.105.3.4.2 Выбрать соответствующее программное средство анализа.

А.105.3.4.3 Выполнить анализ образца ПО с использованием выбранного программного средства анализа.

А.105.3.4.4 Дополнительно к действиям пунктов А.105.3.4.1–А.105.3.4.3 выполнить проверки согласно пунктам А.108.3.5 и А.108.3.10.

Примечание. Допускается совмещение данного действия с проверкой, выполняемой в пункте А.108 (методика Методика № 108).

А.105.3.4.5 Убедиться в возможности проведения динамического анализа образца ПО используемыми программными средствами анализа.

А.105.3.4.6 При необходимости дополнительно (по решению комиссии) выполнить пункты А.105.3.4.1–А.105.3.4.5, для любого другого произвольного образца ПО (нескольких произвольных образцов ПО).

А.105.4 СПО ПТТ считается выдержавшим испытания по п. А.105.3.4.1-А.105.3.4.6 программы и методики испытаний и выполняющим пункты 3.2.8, 3.2.8.6 ТЗ на СЧ ОКР, если программные средства анализа, перечисленные в пункте А.105.3.2 и используемые в пункте А.105.3.4.4, обеспечивают проведение динамического анализа образцов ПО.

А.106 Методика № 106

А.106.1 В данной методике проводится проверка СПО ПТТ на соответствие требованиям пунктов 3.2.8, 3.2.8.7 ТЗ на СЧ ОКР «Амезит-В».

А.106.2 В соответствии с требованиями пунктов 3.2.8, 3.2.8.7 ТЗ на СЧ ОКР «Амезит-В» СПО ПТТ должно обеспечивать автоматизированное распознавание используемых стандартных библиотечных функций по следующему перечню: _getlong, udp_cksum, os_strncpy, os_strncmp, os_strlen, os_strchr, os_strrchr, os_memcmp, os_memset, os_memcpy, scanf, printf, gets.

А.106.3 Проверка обеспечения автоматизированного распознавания используемых стандартных библиотечных функций выполняется с использованием заранее подготовленных файлов образцов ПО, представляющих собой файлы, содержащие стандартные библиотечные функции, перечисленные в пункте А.106.2.

А.106.4 Проверка файлов образцов ПО выполняется с использованием программного средства анализа IDA Pro.

А.106.5 Проверка выполняется в соответствии с документом RU.BATC.00184-01 92 10 «Специальное программное обеспечение подсистемы тестирования телекоммуникационного оборудования. ПО IDA Pro. Руководство пользователя».

А.106.6 Для проведения проверки СПО ПТТ на соответствие предъявляемым требованиям необходимо выполнить действия, описанные ниже.

А.106.6.1 Скопировать образцы ПО в директорию sign_test.

А.106.6.2 Запустить программу IDA Pro.

А.106.6.3 Открыть в программе IDA Pro файл образца ПО, расположенный в директории sign_test, для анализа.

А.106.6.4 Запустить процесс анализа открытого файла образца ПО и дождаться сообщения о его завершении.

А.106.6.5 Просмотреть в списке выявленных функций наличие стандартных библиотечных функций и сравнить их с перечнем стандартных библиотечных функций в исходном коде файла образца ПО. Убедиться в отображении в списке выявленных функций всех стандартных библиотечных функций исходного кода файла образца ПО.

А.106.6.6 Повторить (при необходимости) действия пунктов А.106.6.3–А.106.6.5 для остальных файлов образцов ПО, расположенных в директории sign_test.

А.106.7 СПО ПТТ считается выдержавшим испытания по п. А.106.6.1-А.106.6.6 программы и методики испытаний и выполняющим пункты 3.2.8, 3.2.8.7 ТЗ на СЧ ОКР, если при выполнении пунктов А.106.6.3–А.106.6.6 в файлах образцах ПО обнаружены все стандартные библиотечные функции из приведенного в пункте А.106.2 перечня стандартных библиотечных функций.

А.107 Методика № 107

А.107.1 В данной методике проводится проверка СПО ПТТ на соответствие требованиям пунктов 3.2.8, 3.2.8.8 ТЗ на СЧ ОКР «Амезит-В».

А.107.2 В соответствии с требованиями пунктов 3.2.8, 3.2.8.8 ТЗ на СЧ ОКР «Амезит-В» СПО ПТТ должно обеспечивать сигнатурный анализ потенциально опасных операций по следующему перечню:

- вызов LoadLibraryEx или LoadLibrary с аргументом, содержащим относительный путь;
- вызов функций, работающих с форматной строкой (scanf, printf);
- вызов функций, не контролирующих размер входа при записи в буфер (gets, scanf, strcpy);
- вызов функций, производящих копирование буферов (memcpy, CopyMemory);
- наличие функции без Control Flow Guard;
- наличие модуля без поддержки ASLR;
- наличие страницы с правами на запись и исполнение;
- операции передачи управления по регистру (jmp reg, all reg);
- отсутствие NX-бита;
- наличие отладочной информации в файле.

А.107.3 Проверка обеспечения сигнатурного анализа потенциально опасных операций выполняется с использованием заранее подготовленных образцов ПО, представляющих собой файлы, имеющие в своем составе вызовы перечисленных в пункте А.107.2 функций.

А.107.4 Проверка файлов образцов ПО выполняется с использованием программного средства анализа IDA Pro.

А.107.5 Проверка выполняется в соответствии с документом RU.ВАТС.00184-01 92 10 «Специальное программное обеспечение подсистемы тестирования телекоммуникационного оборудования. ПО IDA Pro. Руководство пользователя».

А.107.6 Для проведения проверки СПО ПТТ на соответствие предъявляемым требованиям необходимо выполнить действия, описанные ниже.

А.107.6.1 Скопировать образцы ПО в директорию critical_test.

А.107.6.2 Запустить программу IDA Pro.

А.107.6.3 Открыть в программе IDA Pro файл образца ПО, расположенный в директории critical_test, для анализа.

А.107.6.4 Запустить процесс анализа открытого файла образца ПО и дождаться сообщения о его завершении.

А.107.6.5 Просмотреть в списке выявленных операций наличие потенциально опасных операций и сравнить их с перечнем операций в исходном коде файла образца ПО. Убедиться в отображении в списке выявленных операций всех потенциально опасных операций исходного кода файла образца ПО.

А.107.6.6 Повторить (при необходимости) действия пунктов А.107.6.3–А.107.6.5 для остальных файлов образцов ПО, расположенных в директории critical_test.

А.107.7 СПО ПТТ считается выдержавшим испытания по п. А.107.6.1-А.107.6.6 программы и методики испытаний и выполняющим пункты 3.2.8, 3.2.8.8 ТЗ на СЧ ОКР, если при выполнении действий в пунктах А.107.6.3–А.107.6.6 обнаружены все потенциально опасные операции из приведенного в пункте А.107.2 перечня.

А.108 Методика № 108

А.108.1 В данной методике проводится проверка СПО ПТТ на соответствие требованиям пунктов 3.2.8, 3.2.8.9 ТЗ на СЧ ОКР «Амезит-В».

А.108.2 В соответствии с требованиями пунктов 3.2.8, 3.2.8.9 ТЗ на СЧ ОКР «Амезит-В» СПО ПТТ должно обеспечивать восстановление логики функционирования и протоколов сетевого взаимодействия программного обеспечения сторонних разработчиков за счет использования следующих механизмов и программных средств:

- осуществление захвата сетевых пакетов, проходящих через сетевой интерфейс, их разбора по уровням модели OSI, статистического анализа массивов пакетов, записи и воспроизведения сетевых сессий, исследования инкапсуляции протоколов, составления собственных сэмплов отдельных пакетов и их последовательностей с использованием программных средств анализа трафика типа Wireshark и Scapy;
- отладки, трассировки, контроля изменения дан-ных, изменения значений переменных в процессе выполнения кода, отслеживания хода выполнения программы, просмотра содержимого ячеек памяти и регистров процессора, поиска ошибок, установки и удаления контрольных точек с использованием программных средств отладки ПО типа WinDBG и gdb;
- динамической инструментации бинарного кода, инжектирования команд в процессе выполнения программы, создания собственных утилит

динамического анализа, Taint-анализа с использованием программных средств динамического анализа типа Intel PIN и Dynamo Rio.

Примечание. В состав программной документации на АПК «Амезит» включить методику восстановления логики функционирования и протоколов сетевого взаимодействия ПО на основе работы с вышеуказанными техническими средствами.

А.108.3 Для проведения проверки СПО ПТТ на соответствие предъявляемым требованиям необходимо выполнить действия, описанные ниже.

А.108.3.1 Проверка обеспечения восстановления логики функционирования и протоколов сетевого взаимодействия ПО сторонних разработчиков за счет использования механизмов и программных средств захвата сетевых пакетов, проходящих через сетевой интерфейс, их разбора по уровням модели OSI, статистического анализа массивов пакетов, записи и воспроизведения сетевых сессий, исследования инкапсуляции протоколов, составления собственных семплов отдельных пакетов и их последовательностей с использованием программных средств анализа трафика типа Wireshark и Scapy выполняется в соответствии с пунктами А.108.3.2–А.108.3.4.

А.108.3.2 Проверка выполняется с использованием рабочей станции (ПЭВМ), подключенной к SPAN-порту сетевого коммутатора, через который циркулируют сетевые потоки между узлами сети и удаленными прикладными серверами. На ПЭВМ должно быть установлено ПО Wireshark и Scapy. В качестве объекта испытания используются два приложения (приложение № 1 – ПО под управлением ОС Android, имеющее в своем составе функцию обмена данными по протоколу HTTPS, приложение № 2 – ПО под управлением ОС Windows, сгенерированное с применением механизмов обфускации).

А.108.3.3 Для проведения проверки необходимо выполнить следующие действия:

А.108.3.3.1 Запустить программные средства анализа трафика Wireshark и Scapy, включить режим мониторинга пакетов на всех сетевых интерфейсах.

А.108.3.3.2 Запустить подготовленные приложения № 1, № 2 и осуществить регистрацию сетевого трафика, генерируемого ими.

А.108.3.3.3 Выполнить разбор записанных пакетов по уровням модели OSI, наблюдая представление этих данных в интерфейсе программ.

А.108.3.3.4 Выполнить статистический анализ массивов пакетов, оценить распределение пакетов по различным протоколам, количественную долю пакетов с определенными характеристиками.

A.108.3.3.5 Выполнить запись и воспроизведение сетевых сессий.

A.108.3.3.6 Провести исследование инкапсуляции протоколов.

A.108.3.3.7 Выполнить формирование собственных семплов отдельных пакетов и их последовательностей.

A.108.3.3.8 Сымитировать информационный обмен клиента и сервера почтового сервиса по протоколам SMTP и/или POP3 и проверить применимость методических указаний по восстановлению логики функционирования и протоколов сетевого взаимодействия ПО сторонних разработчиков применительно к используемым средствам анализа сетевого трафика.

A.108.3.4 Проверка обеспечения восстановления логики функционирования и протоколов сетевого взаимодействия ПО сторонних разработчиков за счет использования механизмов и программных средств захвата сетевых пакетов, проходящих через сетевой интерфейс, их разбора по уровням модели OSI, статистического анализа массивов пакетов, записи и воспроизведения сетевых сессий, исследования инкапсуляции протоколов, составления собственных семплов отдельных пакетов и их последовательностей с использованием программных средств анализа трафика типа Wireshark и Scapy считается выполненной успешно, если успешно выполнены пункты A.108.3.3.1–A.108.3.3.7, а анализ записанного сеанса обмена клиента и сервера почтового сервиса сообщениями по протоколам SMTP и/или POP3 позволил выделить последовательность операций, соответствующих спецификациям RFC на указанные протоколы.

A.108.3.5 Проверка обеспечения восстановления логики функционирования и протоколов сетевого взаимодействия ПО сторонних разработчиков за счет использования механизмов и программных средств отладки, трассировки, контроля изменения данных, изменения значений переменных в процессе выполнения кода, отслеживания хода выполнения программы, просмотра содержимого ячеек памяти и регистров процессора, поиска ошибок, установки и удаления контрольных точек с использованием программных средств отладки ПО типа WinDBG и GNU Debugger проводится в соответствии с пунктами A.108.3.6–A.108.3.9.

A.108.3.6 Проверка выполняется с использованием заранее подготовленного образца ПО, представляющего собой бинарный исполняемый файл с расширением «exe».

A.108.3.7 Проверка выполняется в соответствии с документами RU.BATC.00184-01 92 03 «Специальное программное обеспечение подсистемы тестирования телекоммуникационного оборудования. ПО GNU Debugger. Руководство пользователя», RU.BATC.00184-01 92 04 «Специальное

программное обеспечение подсистемы тестирования телекоммуникационного оборудования. ПО WinDBG. Руководство пользователя».

А.108.3.8 Для проведения проверки необходимо выполнить следующие действия:

А.108.3.8.1 Запустить программу WinDBG.

А.108.3.8.2 Открыть файл образца ПО в программе WinDBG.

А.108.3.8.3 Проверить работоспособность механизмов отладки.

А.108.3.8.4 Проверить работоспособность механизмов трассировки выполнения программы.

А.108.3.8.5 Проверить работоспособность механизмов контроля изменения данных.

А.108.3.8.6 Проверить работоспособность механизмов изменения значений переменных в процессе выполнения кода.

А.108.3.8.7 Проверить работоспособность механизмов отслеживания хода выполнения программы.

А.108.3.8.8 Проверить работоспособность механизмов просмотра содержимого ячеек памяти и регистров процессора.

А.108.3.8.9 Проверить работоспособность механизмов поиска ошибок.

А.108.3.8.10 Проверить работоспособность механизмов установки и удаления контрольных точек.

А.108.3.8.11 Выполнить пункты А.108.3.8.1–А.108.3.8.10 с использованием программы GNU Debugger.

А.108.3.9 Проверка обеспечения восстановления логики функционирования и протоколов сетевого взаимодействия ПО сторонних разработчиков за счет использования механизмов и программных средств отладки, трассировки, контроля изменения данных, изменения значений переменных в процессе выполнения кода, отслеживания хода выполнения программы, просмотра содержимого ячеек памяти и регистров процессора, поиска ошибок, установки и удаления контрольных точек с использованием программных средств отладки ПО типа WinDBG и GNU Debugger считается выполненной успешно, если пункты А.108.3.8.1–А.108.3.8.11 выполнены успешно.

А.108.3.10 Проверка обеспечения восстановления логики функционирования и протоколов сетевого взаимодействия ПО сторонних разработчиков за счет использования механизмов и программных средств динамической инструментации бинарного кода, инжектирования команд в процессе выполнения программы, создания собственных утилит динамического анализа, Taint-анализа с использованием программных средств динамического

анализа типа Intel Pin и DynamoRIO проводится в соответствии с пунктами А.108.3.11–А.108.3.14.

А.108.3.11 Проверка выполняется с использованием заранее подготовленного образца ПО, представляющего собой бинарный исполняемый файл с расширением «exe».

А.108.3.12 Проверка проводится в соответствии с документами RU.BATC.00184-01 92 12 «Специальное программное обеспечение подсистемы тестирования телекоммуникационного оборудования. ПО Intel PIN. Руководство по эксплуатации», RU.BATC.00184-01 92 13 «Специальное программное обеспечение подсистемы тестирования телекоммуникационного оборудования. ПО DynamoRIO. Руководство по эксплуатации».

А.108.3.13 Для проведения проверки необходимо выполнить следующие действия:

А.108.3.13.1 Запустить программное средство Intel Pin.

А.108.3.13.2 Открыть файл образца ПО в программе Intel Pin.

А.108.3.13.3 Проверить отсутствие информации об ошибках и сбоях при работе механизмов динамической инструментации бинарного кода.

А.108.3.13.4 Проверить отсутствие информации об ошибках и сбоях при работе механизмов инжектирования команд в процессе выполнения программы.

А.108.3.13.5 Проверить отсутствие информации об ошибках и сбоях при работе механизмов создания собственных утилит динамического анализа, Taint-анализа.

А.108.3.13.6 Выполнить пункты А.108.3.13.1–А.108.3.13.5 с использованием программы DynamoRIO.

А.108.3.14 Проверка обеспечения восстановления логики функционирования и протоколов сетевого взаимодействия ПО сторонних разработчиков за счет использования механизмов и программных средств динамической инструментации бинарного кода, инжектирования команд в процессе выполнения программы, создания собственных утилит динамического анализа, Taint-анализа с использованием программных средств динамического анализа типа Intel Pin и DynamoRIO считается выполненной успешно, если во время проверок, выполненных в пунктах А.108.3.13.1–А.108.3.13.6, информация об ошибках и сбоях отсутствует.

А.108.3.15 Проверка представления в составе программной документации на СПО «Амезит-В» методик восстановления логики функционирования и протоколов сетевого взаимодействия ПО осуществляется путем просмотра комплекта документации, представленной на испытание, на наличие в ней

указанных методик и оценки содержания данных методик на возможность их применения при проведении проверок с использованием программ Wireshark и Scapy, WinDBG и GNU Debugger, Intel Pin и DynamoRIO.

А.108.3.16 Проверка считается выполненной успешно, если в комплекте документации, представленной на испытание, присутствуют методические указания по восстановлению логики функционирования и протоколов сетевого взаимодействия ПО, а их содержание обеспечивает проведение с помощью программных средств Wireshark и Scapy, WinDBG и GNU Debugger, Intel Pin и DynamoRIO восстановление логики функционирования и протоколов сетевого взаимодействия ПО.

А.108.4 СПО ПТТ считается выдержавшим испытания по п. А.108.3.1-А.108.3.16 программы и методики испытаний и выполняющим пункты 3.2.8, 3.2.8.9 ТЗ на СЧ ОКР, если выполнены условия в пунктах А.108.3.4, А.108.3.9, А.108.3.14, А.108.3.16.

А.109 Методика № 109

А.109.1 В данной методике проводится проверка СПО ПТТ на соответствие требованиям пунктов 3.2.8, 3.2.8.10 ТЗ на СЧ ОКР «Амезит-В».

А.109.2 В соответствии с требованиями пунктов 3.2.8, 3.2.8.10 ТЗ на СЧ ОКР «Амезит-В» СПО ПТТ должно обеспечивать автоматизированную проверку СПО АПК «Амезит» САВЗ.

А.109.3 Проверка выполняется с использованием двух предварительно подготовленных контрольных образцов ПО: образец ПО № 1 – тестовый файл, содержащий вредоносный код; образец ПО № 2 – безопасный файл произвольного формата. В ходе проверки дополнительно могут быть использованы образцы ПО, заведомо содержащие вредоносный код.

А.109.4 Для проведения проверки СПО ПТТ на соответствие предъявляемым требованиям необходимо выполнить действия, описанные ниже.

А.109.4.1 Запустить ПО анализатора трафика.

А.109.4.2 Запустить ПО VMware Client, проверить включение ВМ управления и ВМ САВЗ, убедиться в отключении всех ВМ стенда антивирусного контроля от сети Интернет, убедиться в работе антивирусных программ.

А.109.4.3 Запустить (перезапустить) управляющее СПО (launcher.py) на ВМ управления (перезапуск выполняется с целью формирования новых журналов регистрации в случае, если управляющее СПО было запущено ранее).

А.109.4.4 Запустить обозреватель и выполнить подключение к веб-интерфейсу СПО стенда антивирусного контроля.

А.109.4.5 Выбрать контрольный образец ПО № 1 и запустить процедуру его проверки САВЗ.

А.109.4.6 Дождаться окончания проверки, просмотреть результаты в отчете, представленном в табличном виде и в виде графика, убедиться в выявлении САВЗ вредоносного кода в образце ПО № 1, убедиться в наличии данных от всех САВЗ, включенных в состав СПО стенда антивирусного контроля.

А.109.4.7 Записать (скопировать в текстовый файл) значение хеш образца ПО № 1.

А.109.4.8 Выбрать контрольный образец ПО № 2 и запустить процедуру его проверки САВЗ.

А.109.4.9 Дождаться окончания проверки, просмотреть результаты в отчете, представленном в табличном виде и в виде графика, убедиться в безопасности образца ПО № 2, убедиться в наличии данных от всех САВЗ, включенных в состав СПО стенда антивирусного контроля.

А.109.4.10 Выбрать один из дополнительных образцов ПО и запустить процедуру его проверки САВЗ (пункты А.109.4.10 и А.109.4.11 могут быть пропущены или выполнены по решению комиссии).

А.109.4.11 Дождаться окончания проверки, просмотреть результаты в отчете, представленном в табличном виде и в виде графика, убедиться в выявлении САВЗ вредоносного кода в образце ПО, убедиться в наличии данных от всех САВЗ, включенных в состав СПО стенда антивирусного контроля.

А.109.4.12 Составить расписание проверки образца ПО № 1 с использованием значения хеш, записанного в пункте А.109.4.7, указав время начала проверки через пять минут от текущего времени и интервал проверки – один день.

А.109.4.13 Дождаться выполнения проверки образца ПО № 1 по расписанию, просмотреть результаты в отчете, представленном в табличном виде и в виде графика, убедиться в идентичности результатов проверок, выполненных в ручном и автоматизированном режимах.

А.109.4.14 Убедиться в запуске проверки по расписанию в указанное время (время проверки отображается в отчете и в журналах регистрации событий).

А.109.4.15 Установить для образца ПО № 1 новое расписание. Убедиться в отображении диалогового окна, открывающегося перед сохранением нового расписания, с информацией о предыдущем расписании.

А.109.4.16 Просмотреть журналы регистрации событий, убедиться в отсутствии подключений к сети Интернет во время и после проведения проверок, в отсутствии критических ошибок, которые могли возникнуть в процессе работы СПО стенда антивирусного контроля (ошибки, возникшие по причинам, не связанным с работой проверяемой программы, не являются признаком неработоспособности СПО стенда антивирусной контроля).

А.109.5 СПО ПТТ считается выдержавшим испытания по п. А.109.4.2-А.109.4.16 программы и методики испытаний и выполняющим пункты 3.2.8, 3.2.8.10 ТЗ на СЧ ОКР, если в ходе работы СПО стенда антивирусного контроля:

- в тестовом образце ПО № 1 (и дополнительных образцах ПО) выявлено наличие вредоносного кода;
- в тестовом образце ПО № 2 вредоносный код не обнаружен;
- в сформированных отчетах присутствуют результаты проверок всех САВЗ, включенных в состав стенда;
- проверка образца ПО № 1 выполнена в соответствии с заданным в расписании временем и при установке нового расписания отображается информация о предыдущем расписании;
- результаты проверок образца ПО № 1, выполненные в ручном и автоматизированном режиме, идентичны;
- в процессе и после выполнения проверок отсутствовало соединение с сетью Интернет, передача данных третьей стороне не происходила;
- отсутствуют программные сбои (критические ошибки).

А.110 Методика № 110

А.110.1 В данной методике проводится проверка СПО ПТТ на соответствие требованиям пунктов 3.2.8, 3.2.8.11 ТЗ на СЧ ОКР «Амезит-В».

А.110.2 В соответствии с требованиями пунктов 3.2.8, 3.2.8.11 ТЗ на СЧ ОКР «Амезит-В» СПО ПТТ должно обеспечивать автоматизированное обновление баз вирусных сигнатур из доверенных источников.

А.110.3 Для проведения проверки СПО ПТТ на соответствие предъявляемым требованиям необходимо выполнить действия, описанные ниже.

А.110.3.1 Запустить ПО анализатора трафика.

А.110.3.2 Запустить ПО VMware Client, проверить включение ВМ управления и ВМ САВЗ, убедиться в отключении ВМ от сети Интернет, убедиться в работе антивирусных программ.

А.110.3.3 Задать время обновления в конфигурационном файле config.py и согласовать указанное время с временем обновления САВЗ (в каждом САВЗ установить требуемое время и условия обновления).

А.110.3.4 Запустить (перезапустить) управляющее СПО (launcher.py) на ВМ управления (перезапуск выполняется с целью принятия измененных данных конфигурационного файла и формирования новых журналов регистрации событий в случае, если управляющее СПО было запущено ранее).

А.110.3.5 Дождаться времени начала обновления САВЗ. Убедиться в автоматическом подключении ВМ к сети Интернет после их восстановления из заранее созданных образов (снапшотов).

А.110.3.6 С помощью анализатора трафика проконтролировать IP-адреса, к которым обращаются САВЗ для обновления.

А.110.3.7 Дождаться завершения процедуры обновления (по умолчанию продолжительность обновления составляет один час). Убедиться в автоматическом отключении сети Интернет по завершении процедуры обновления.

А.110.3.8 Убедиться в принадлежности IP-адресов, с которых осуществляется обновление антивирусных баз САВЗ, разработчикам антивирусных программ с помощью сервиса Whois.

Примечания:

1. IP-адреса серверов обновления предустановлены разработчиками САВЗ и не могут быть изменены штатными средствами антивирусных программ.
2. Обновление антивирусных баз и САВЗ может быть выполнено с задействованием основных или «зеркальных» серверов разработчиков антивирусных программ.
3. Защита от изменения IP-адресов серверов, задействованных в процессе обновления антивирусных баз и САВЗ, обеспечивается проведением процедуры обновления с использованием образов ВМ САВЗ, не подвергавшихся воздействию вредоносного ПО.

А.110.3.9 Перейти на вкладку «Events» ПО VMware Client и просмотреть журналы регистрации событий для каждого САВЗ. Убедиться в наличии сообщений:

- Virtual machine disks consolidation succeeded (консолидация дисков виртуальной машины выполнена успешно).

- Reconfigured virtual machine (реконфигурация виртуальной машины – отключение ВМ от сети Интернет);
- Reconfigured virtual machine (реконфигурация виртуальной машины – подключение ВМ к сети Интернет);
- The execution state of the virtual machine has been reverted to the state of cnapshot temp_snap,with ID [номер] (виртуальная машина восстановлена из снапшота (резервного образа) temp_snap с ID [номер], где [номер] – номер снапшота);
- Reconfigured virtual machine (реконфигурация виртуальной машины – подготовка ВМ к восстановлению).

Примечание. Обновление некоторых САВЗ может быть не выполнено по причине отсутствия на момент проведения проверки изменений, внесенных разработчиком в антивирусные базы.

А.110.3.10 Перейти на вкладку «Console» ПО VMware Client и для каждого САВЗ убедиться в отсутствии сообщений о необходимости обновления.

А.110.4 СПО ПТТ считается выдержавшим испытания по п. А.110.3.1-А.110.3.10 программы и методики испытаний и выполняющим пункты 3.2.8, 3.2.8.11 ТЗ на СЧ ОКР, если:

- обновление антивирусных баз и САВЗ выполняется в три этапа:
    1) восстановление ВМ САВЗ из ранее созданных образов (снапшотов);
    2) обновление антивирусных баз и САВЗ из источников, принадлежащих разработчикам антивирусных программ;
    3) создание образов ВМ САВЗ (снапшотов) с обновленными антивирусными программами;
- обновление антивирусных баз и САВЗ выполняется в указанное время и с установленной продолжительностью;
- подключение ВМ САВЗ к сети Интернет осуществляется только после восстановления ВМ из ранее созданных образов (снапшотов) и только на время обновления антивирусных баз и САВЗ.

А.111 Методика № 111

А.111.1 В данной методике проводится проверка СПО ПТТ на соответствие требованиям пунктов 3.2.8, 3.2.8.12 ТЗ на СЧ ОКР «Амезит-В».

А.111.2 В соответствии с требованиями пунктов 3.2.8, 3.2.8.12 ТЗ на СЧ ОКР «Амезит-В» СПО ПТТ должно обеспечивать автоматизированный поиск внесенных изменений в программный код системного и прикладного ПО сторонних разработчиков при его модификации.

Примечание. Все программное обеспечение включает 32- и 64-разрядные версии при их наличии.

А.111.3 Для проведения проверки СПО ПТТ на соответствие предъявляемым требованиям необходимо выполнить действия, описанные ниже.

А.111.3.1 В директории с тестовыми наборами данных diff_test создать вложенные каталоги, разместить в них контрольные файлы v1.c, v2.c (или иные), а также их скомпилированные версии (файл v2 является модифицированной версией файла v1).

А.111.3.2 Используя программное средство BinDiff, выполнить поиск изменений в исполняемых файлах в соответствии с указаниями, приведенными в документе RU.BATC.00184-01 34 05 «Специальное программное обеспечение подсистемы тестирования телекоммуникационного оборудования. ПО BinDiff и Diaphora. Руководство оператора».

А.111.3.3 Проконтролировать полноту найденных изменений.

А.111.3.4 Используя программное средство Daiphora, выполнить поиск изменений в исполняемых файлах в соответствии с указаниями, приведенными в документе RU.BATC.00184-01 34 05 «Специальное программное обеспечение подсистемы тестирования телекоммуникационного оборудования. ПО BinDiff и Diaphora. Руководство оператора».

А.111.3.5 Проконтролировать полноту найденных изменений.

А.111.3.6 При необходимости выполнить аналогичные операции с дополнительными тестовыми образцами.

А.111.4 СПО ПТТ считается выдержавшим испытания по п. А.111.3.1-А.111.3.6 программы и методики испытаний и выполняющим пункты 3.2.8, 3.2.8.12 ТЗ на СЧ ОКР, если при выполнении проверки найдены переименованные функции и обнаружены измененные участки кода (добавленные и удаленные конструкции).

А.112 Методика № 112

А.112.1 В данной методике проводится проверка СПО ПТТ на соответствие требованиям пунктов 3.2.8, 3.2.8.13 ТЗ на СЧ ОКР «Амезит-В».

А.112.2 В соответствии с требованиями пунктов 3.2.8, 3.2.8.13 ТЗ на СЧ ОКР «Амезит-В» СПО ПТТ должно обеспечивать моделирование угроз информационной безопасности на основе разрабатываемого образца СПО, имитирующего поведение широко распространенных компьютерных вирусов (троянских программ) и обеспечивающего:

- функционирование под управлением операционных систем семейства Windows на 32– и 64-разрядных процессорах;
- удаленное управление через промежуточный узел обмена данными и командами по защищенному протоколу (с использованием собственной системы управления и ретрансляции команд);
- противодействие обнаружению локальными средствами защиты при установке в систему;
- уникальность бинарного файла каждого образца и реализацию алгоритмов модификации исполняемого файла, позволяющие минимизировать возможность занесения его в базы данных антивирусных средств;
- противодействие обнаружению локальными средствами защиты после установки в систему;
- сбор общей информации о системе и отправку ее на сервер управления;
- сбор информации о нажатиях клавиш на клавиатуре;
- сбор информации о файловой системе и передачу заданных файлов в центр управления, а также передачу файлов из центра управления в файловую систему;
- выполнение снимков экрана с передачей информации в центр управления;
- поддержку модульной структуры, позволяющей динамически изменять функциональность образца.

А.112.3 Для проведения проверки СПО ПТТ на соответствие предъявляемым требованиям необходимо выполнить действия, описанные ниже.

А.112.3.1 Проверка обеспечения функционирования под управлением ОС семейства Windows на 32- и 64-разрядных процессорах выполняется в ходе проверок, проводимых в соответствии с пунктами А.112.3.3–А.112.3.39 с задействованием целевых ПЭВМ, работающих под управлением ОС Windows 7 x32 и Windows 10 x64.

А.112.3.2 Проверка обеспечения функционирования под управлением операционных систем семейства Windows на 32- и 64-разрядных процессорах считается выполненной успешно, если проверки, приведенные в пунктах А.112.3.3–А.112.3.39, пройдены успешно, при этом в ходе их выполнения были задействованы целевые ПЭВМ, работающие под управлением как ОС Windows 7 x32, так и ОС Windows 10 x64.

А.112.3.3 Проверка обеспечения удаленного управления через промежуточный узел обмена данными и командами по защищенному

протоколу (с использованием собственной системы управления и ретрансляции команд) выполняется в соответствии с пунктами А.112.3.4–А.112.3.6.

А.112.3.4 Проверка выполняется с использованием инфраструктуры, состоящей из АРМ управления и компонентов, имитирующих: сервер управления, промежуточный сервер, целевую ПЭВМ, работающую под управлением ОС Windows (версии 7 x32 или версии 10 x64), с установленными на указанные компоненты соответствующими программными модулями СПО «Спутник», и узел контроля трафика.

А.112.3.5 Для проведения проверки необходимо выполнить следующие действия:

А.112.3.5.1 Запустить на узле контроля трафика ПО анализа трафика, убедиться в его подключении к промежуточному серверу.

А.112.3.5.2 Запустить на АРМ управления обозреватель, выполнить подключение к веб-интерфейсу СПО «Спутник», создать задачу просмотра перечня директорий целевой ПЭВМ, дождаться изменения статуса задачи на «Выполнено».

А.112.3.5.3 Убедится с помощью ПО анализа трафика в отсутствии незашифрованных пакетов, передаваемых через промежуточный сервер в процессе обмена данными между сервером управления и целевой ПЭВМ.

А.112.3.6 Проверка обеспечения возможности удаленного управления через промежуточный узел обмена данными и командами по защищенному протоколу (с использованием собственной системы управления и ретрансляции команд) считается выполненной успешно, если:

- операция просмотра перечня директорий целевой ПЭВМ завершена корректно;
- ПО анализа трафика не зарегистрировало передачу команд и данных в открытом (незашифрованном) виде в процессе их ретрансляции через промежуточный сервер.

А.112.3.7 Проверка обеспечения противодействия обнаружению локальными средствами защиты при установке в систему выполняется в соответствии с пунктами А.112.3.8–А.112.3.10.

А.112.3.8 Проверка выполняется с использованием установочного файла модуля «agent» СПО «Спутник», компонента, имитирующего целевую ПЭВМ, работающую под управлением ОС Windows (версии 7 x32 или версии 10 x64) с установленным САВЗ.

Примечание. Для проведения проверки в качестве целевых ПЭВМ, с установленными на них САВЗ, допускается использование компонентов СПО стенда антивирусного контроля.

А.112.3.9 Для проведения проверки необходимо выполнить следующие действия:

А.112.3.9.1 Загрузить установочный файл модуля «agent» СПО «Спутник» на целевую ПЭВМ, работающую под управлением ОС Windows (версии 7 x32 или версии 10 x64), с установленным САВЗ.

А.112.3.9.2 Выполнить проверку САВЗ установочного файла модуля «agent» и убедиться в отсутствии угроз безопасности или в их наличии в соответствии с эксплуатационными ограничениями на применение СПО «Спутник».

А.112.3.10 Проверка обеспечения противодействия обнаружению локальными средствами защиты при установке в систему считается пройденной успешно, если САВЗ не обнаруживает в установочном файле модуля «agent» угроз безопасности либо обнаружение угрозы безопасности происходит в соответствии с эксплуатационными ограничениями на применение СПО «Спутник».

А.112.3.11 Проверка обеспечения уникальности бинарного файла каждого семпла и реализации алгоритмов модификации исполняемого файла, позволяющих минимизировать возможность занесения его в базы данных антивирусных средств, выполняется в соответствии с пунктами А.112.3.12–А.112.3.14.

А.112.3.12 Проверка выполняется с использованием образца файла, содержащего вредоносный код, АРМ оператора, компонентов, имитирующих сервер управления и целевую ПЭВМ, работающую под управлением ОС Windows (версии 7 x32 или версии 10 x64), с установленным САВЗ.

Примечание. Для проведения проверки в качестве целевых ПЭВМ с установленными на них САВЗ допускается использование компонентов СПО стенда антивирусного контроля.

А.112.3.13 Для проведения проверки необходимо выполнить следующие действия:

А.112.3.13.1 Запустить на АРМ оператора программный модуль криптора, обеспечивающего уникальность бинарного файла.

А.112.3.13.2 В качестве входных данных передать модулю криптора заранее подготовленный образец файла, который содержит вредоносный код и определяется антивирусными средствами как представляющий угрозу безопасности.

А.112.3.13.3 Сгенерировать не менее пяти бинарных семплов, рассчитать их контрольные суммы с использованием одного криптографического

алгоритма и сравнить полученные значения контрольных сумм. Отметить различие полученных значений контрольных сумм.

А.112.3.13.4 Проверить каждый семпл САВЗ, которое изначально определяло файл подготовленного образца как представляющий угрозу безопасности, и убедиться в отсутствии угроз безопасности.

А.112.3.14 Проверка обеспечения уникальности бинарного файла каждого семпла и реализации алгоритмов модификации исполняемого файла, позволяющих минимизировать возможность занесения его в базы данных антивирусных средств, считается выполненной успешно, если:

- контрольные суммы сгенерированных аналогичным образом семплов отличаются друг от друга;
- сгенерированные семплы не определяются САВЗ как представляющие угрозу безопасности.

А.112.3.15 Проверка обеспечения противодействия после установки в систему обнаружению локальными средствами защиты выполняется в соответствии с пунктами А.112.3.16–А.112.3.18.

А.112.3.16 Проверка выполняется с использованием установочного файла модуля «agent» СПО «Спутник», компонента, имитирующего целевую ПЭВМ, работающую под управлением ОС Windows (версии 7 x32 или версии 10 x64) с установленным САВЗ.

Примечание. Для проведения проверки в качестве целевых ПЭВМ с установленными на них САВЗ допускается использование компонентов СПО стенда антивирусного контроля.

А.112.3.17 Для проведения проверки необходимо выполнить следующие действия:

А.112.3.17.1 Обновить антивирусную базу САВЗ (если не обновлена ранее) на целевой ПЭВМ, работающей под управлением ОС Windows (версии 7 x32 или версии 10 x64).

А.112.3.17.2 Отключить целевую ПЭВМ от сети Интернет.

А.112.3.17.3 Установить на целевую ПЭВМ программный модуль «agent» СПО «Спутник» и запустить САВЗ в режиме полной проверки компьютера. Дождаться окончания проверки и убедиться в отсутствии угроз безопасности или в их наличии в соответствии с эксплуатационными ограничениями на применение СПО «Спутник».

А.112.3.18 По окончании проверки обязательно привести целевую ПЭВМ и установленное на нее САВЗ в состояние, предотвращающее возможную передачу третьей стороне результатов выполненной проверки.

А.112.3.19 Проверка обеспечения противодействия после установки в систему обнаружению локальными средствами защиты считается выполненной успешно, если САВЗ не обнаруживает угроз безопасности либо обнаружение угроз безопасности происходит в соответствии с эксплуатационными ограничениями на применение СПО «Спутник».

А.112.3.20 Проверка обеспечения сбора общей информации о системе и отправки ее на сервер управления выполняется в соответствии с пунктами А.112.3.21–А.112.3.23.

А.112.3.21 Проверка выполняется с использованием инфраструктуры, состоящей из АРМ управления и компонентов, имитирующих: сервер управления, промежуточный сервер и целевую ПЭВМ, работающую под управлением ОС Windows (версии 7 x32 или версии 10 x64), с установленными на указанные компоненты соответствующими программными модулями СПО «Спутник».

А.112.3.22 Для проведения проверки необходимо выполнить следующие действия:

А.112.3.22.1 С АРМ управления отправить программному модулю «agent» СПО «Спутник» команду на сбор и отправку на сервер управления данных о целевой ПЭВМ.

А.112.3.22.2 Просмотреть на АРМ управления полученные данные о наименовании ПЭВМ, наименовании учетной записи пользователя, типе и версии ОС, IP адресе узла и сравнить их с соответствующими данными целевой ПЭВМ. Убедиться в идентичности полученных данных и данных целевой ПЭВМ.

А.112.3.23 Проверка обеспечения сбора общей информации о системе и отправки ее на сервер управления считается выполненной успешно, если данные о наименовании ПЭВМ, наименовании учетной записи пользователя, типе и версии ОС и IP адресе узла, полученные сервером управления, идентичны аналогичным данным целевой ПЭВМ.

А.112.3.24 Проверка обеспечения сбора информации о нажатиях клавиш на клавиатуре выполняется в соответствии с пунктами А.112.3.25–А.112.3.27.

А.112.3.25 Проверка выполняется с использованием инфраструктуры, состоящей из АРМ управления и компонентов, имитирующих сервер управления, промежуточный сервер и целевую ПЭВМ, работающую под управлением ОС Windows (версии 7 x32 или версии 10 x64), с установленными на указанные компоненты соответствующими программными модулями СПО «Спутник».

А.112.3.26 Для проведения проверки необходимо выполнить следующие действия:

А.112.3.26.1 Выполнить на клавиатуре целевой ПЭВМ набор произвольного текста, нажать клавиши навигации, например стрелка вниз, стрелка влево, PageUp и т.п. (набор нажимаемых клавиш может быть подготовлен заранее, или записан в процессе нажатия на произвольные клавиши).

А.112.3.26.2 Просмотреть на АРМ управления полученные данные о нажатых клавишах и сравнить перечень клавиш, нажатых на целевой ПЭВМ, с перечнем клавиш, полученных сервером управления.

А.112.3.27 Проверка обеспечения сбора информации о нажатиях клавиш на клавиатуре считается выполненной успешно, если данные о перечне и последовательности нажатия клавиш, полученные сервером управления, соответствуют перечню и последовательности нажатия клавиш на целевой ПЭВМ.

А.112.3.28 Проверка обеспечения сбора информации о файловой системе и передачи заданных файлов в центр управления, а также передачи файлов из центра управления в файловую систему выполняется в соответствии с пунктами А.112.3.29–А.112.3.31.

А.112.3.29 Проверка выполняется с использованием инфраструктуры, состоящей из АРМ управления и компонентов, имитирующих сервер управления, промежуточный сервер и целевую ПЭВМ, работающую под управлением ОС Windows (версии 7 x32 или версии 10 x64), с установленными на указанные компоненты соответствующими программными модулями СПО «Спутник».

А.112.3.30 Для проведения проверки необходимо выполнить следующие действия:

А.112.3.30.1 На АРМ управления выполнить операцию получения списка файлов целевой ПЭВМ, просмотреть полученный перечень директорий и файлов, убедиться в его корректном отображении.

А.112.3.30.2 Выбрать произвольный файл из произвольной директории целевой ПЭВМ и передать команду на его загрузку на сервер управления.

А.112.3.30.3 Дождаться загрузки файла. Сравнить файл, загруженный на сервер управления, с исходным файлом, расположенным в файловой системе целевой ПЭВМ, и убедиться в их идентичности.

А.112.3.30.4 Выбрать произвольный файл в произвольной директории сервера управления и передать команду на его загрузку в заданную директорию целевой ПЭВМ.

А.112.3.30.5 Дождаться загрузки файла, убедиться в загрузке файла в заданную директорию целевой ПЭВМ. Сравнить файл, загруженный на целевую ПЭВМ, с исходным файлом и убедиться в их идентичности.

А.112.3.31 Проверка обеспечения сбора информации о файловой системе и передачи заданных файлов в центр управления, а также передачи файлов из центра управления в файловую систему считается выполненной успешно, если:

- корректно отображается список директорий и файлов целевой ПЭВМ;
- файлы, передающиеся между сервером управления и целевой ПЭВМ, идентичны;
- файл, переданный на целевую ПЭВМ, загружается в заданную оператором директорию.

А.112.3.32 Проверка обеспечения выполнения снимков экрана с передачей информации в центр управления выполняется в соответствии с пунктами
А.112.3.33–А.112.3.35.

А.112.3.33 Проверка выполняется с использованием инфраструктуры, состоящей из АРМ управления и компонентов, имитирующих сервер управления, промежуточный сервер и целевую ПЭВМ, работающую под управлением ОС Windows (версии 7 x32 или версии 10 x64), с установленными на указанные компоненты соответствующими программными модулями СПО «Спутник».

А.112.3.34 Для проведения проверки необходимо с АРМ управления передать команду на выполнение снимков экрана целевой ПЭВМ, дождаться завершения операции и убедиться в создании в галерее изображений (all screenshots) новых файлов со снимками экрана целевой ПЭВМ. Просмотреть полученные изображения и убедиться в корректности их отображения.

А.112.3.35 Проверка обеспечения выполнения снимков экрана с передачей информации в центр управления считается выполненной успешно, если после выдачи команды на выполнение снимков получено корректное изображение экрана целевой ПЭВМ.

А.112.3.36 Проверка обеспечения поддержки модульной структуры, позволяющей динамически изменять функциональность образца, выполняется в соответствии с пунктами А.112.3.37–А.112.3.39.

А.112.3.37 Проверка выполняется с использованием инфраструктуры, состоящей из АРМ управления и компонентов, имитирующих сервер управления, промежуточный сервер и целевую ПЭВМ, работающую под управлением ОС Windows (версии 7 x32 или версии 10 x64), с установленными

на указанные компоненты соответствующими программными модулями СПО «Спутник».

А.112.3.38 Для проведения проверки необходимо загрузить тестовый модуль на целевую ПЭВМ, запустить функцию установленного модуля с заданными параметрами, проверить корректность выполнения заданной функции.

А.112.3.39 Проверка обеспечения поддержки модульной структуры, позволяющей динамически изменять функциональность образца, считается выполненной успешно, если:

- ядро модуля «agent» СПО «Спутник» позволяет производить установку дополнительных модулей, загружаемых на целевую ПЭВМ по сети Интернет;
- ядро модуля «agent» СПО «Спутник» корректно выполняет функции загруженного модуля.

А.112.4 СПО ПТТ считается выдержавшим испытания по п. А.112.3.1-А.112.3.39 программы и методики испытаний и выполняющим пункты 3.2.8, 3.2.8.13 ТЗ на СЧ ОКР, если выполнены условия пунктов А.112.3.2, А.112.3.6, А.112.3.10, А.112.3.14, А.112.3.19, А.112.3.23, А.112.3.27, А.112.3.31, А.112.3.35, А.112.3.39.

А.113 Методика № 113

А.113.1 В данной методике проводится проверка СПО ПТТ на соответствие требованиям пунктов 3.2.8, 3.2.8.14 ТЗ на СЧ ОКР «Амезит-В».

А.113.2 В соответствии с требованиями пунктов 3.2.8, 3.2.8.14 ТЗ на СЧ ОКР «Амезит-В» СПО ПТТ должно обеспечивать моделирование элементов и сегментов компьютерных сетей автономного сегмента для тестирования функциональных возможностей средств защиты информации.

Примечание. Варианты и функциональные возможности моделирования угроз информационной безопасности определяются по результатам эскизного проектирования и согласовываются с головным исполнителем.

А.113.3 Для проведения проверки СПО ПТТ на соответствие предъявляемым требованиям необходимо выполнить действия, описанные ниже.

А.113.3.1 Запустить ПО VMware ESXi, убедиться в подключении всех ВМ сети LAN № 1 к виртуальному шлюзу № 1 (при отсутствии подключения – подключить), убедиться в подключении всех ВМ сети LAN № 2 к виртуальному шлюзу № 2 (при отсутствии подключения – подключить), просмотреть и записать IP-адреса серверов № 1 и № 2 сети Internet, запустить (перезапустить) все ВМ.

А.113.3.2 Осуществить вход в одну из ВМ сети LAN № 1, запустить на данной ВМ окно командной строки (cmd.exe) и выполнить в нем команду ipconfig.

А.113.3.3 Убедиться в отображении IP-адресов всех ПЭВМ, входящих в сеть LAN № 1.

А.113.3.4 Выполнить команду ping [IP-адрес], где [IP-адрес] – IP-адрес одного из серверов (№ 1 или № 2) сети Internet.

А.113.3.5 Убедиться в наличии подключения выбранной ВМ сети LAN № 1 к серверам сети Internet.

А.113.3.6 Осуществить вход в одну из ВМ сети LAN № 2, запустить на данной ВМ окно командной строки (cmd.exe) и выполнить в нем команду ipconfig.

А.113.3.7 Убедиться в отображении IP-адресов всех ПЭВМ, входящих в сеть LAN № 2.

А.113.3.8 Выполнить команду ping [IP-адрес], где [IP-адрес] – IP-адрес одного из серверов (№ 1 или № 2) сети Internet.

А.113.3.9 Убедиться в наличии подключения выбранной ВМ сети LAN № 2 к серверам сети Internet.

А.113.4 СПО ПТТ считается выдержавшим испытания по п. А.113.3.1-А.113.3.9 программы и методики испытаний и выполняющим пункты 3.2.8, 3.2.8.14 ТЗ на СЧ ОКР, если:

- ВМ сети LAN № 1 образуют единую сеть, моделирующую локальную сеть организации;
- ВМ сети LAN № 2 образуют единую сеть, моделирующую локальную сеть управляющих АРМ;
- в наличии ВМ (серверы № 1 и № 2), моделирующие технические ресурсы ГИС ОП Интернет;
- в пунктах А.113.3.5, А.113.3.9 присутствует соединение ВМ сети LAN № 1 и ВМ сети LAN № 2 к серверам № 1 и № 2 сети Internet, моделирующие подключение ПЭВМ сетей LAN № 1 и LAN № 2 к ГИС ОП Интернет.

А.114 Методика № 114

А.114.1 В данной методике проводится проверка СПО ПХД на соответствие требованиям пунктов 3.2.9, 3.2.9.1 ТЗ на СЧ ОКР «Амезит-В».

А.114.2 В соответствии с требованиями пунктов 3.2.9, 3.2.9.1 ТЗ на СЧ ОКР «Амезит-В» СПО ПХД должно обеспечивать хранение информации, собранной с помощью подсистем ПМС и ПКС со следующими сроками:

- для СПО мониторинга сети Интернет и СМИ:
- хранение информации из социальных сетей – 1 месяц;
- хранение информации из интернет СМИ и веб-сайтов – 2 месяца;
- для СПО контроля сообщений автономного сегмента:
- хранение метаданных о сессиях пользователей – 2 недели;
- хранение файлов из сессии пользователей – 2 месяца.

Объем хранимой информации должен быть не менее 16 Тб.

Примечание. Сроки хранения данных, выбор хранимой информации, объем хранимой информации и выбор удаляемой информации по истечении срока хранения данных должны быть настраиваемыми.

А.114.3 Для проведения проверки СПО ПХД на соответствие предъявляемым требованиям необходимо выполнить действия, описанные ниже.

А.114.3.1 На рабочем столе АРМ оператора запустить обозреватель.

А.114.3.2 В адресной строке ввести адрес сервера приложений и нажать на клавишу «Enter». Адрес сервера приложений уточняется после установки и настройки СПО ПХД согласно документу RU.BATC.00185-01 32 01 «Специальное программное обеспечение подсистемы хранения данных. Руководство системного программиста». Откроется страница авторизации.

А.114.3.3 На странице авторизации ввести аутентификационные данные (логин: admin, пароль: password) и нажать на кнопку «Войти». Откроется страница хранимых публикаций в ПХД. Описание интерфейса СПО ПХД приведено в документе RU.BATC.00185-01 34 01 «Специальное программное обеспечение подсистемы хранения данных. Руководство оператора».

А.114.3.4 В верхней части страницы в панели навигации нажать на «Файлы». Открывается страница с каталогами в файловом хранилище.

А.114.3.5 В рабочей области страницы «Файлы» выбрать каталог «media». На странице отобразятся медиафайлы (видео, аудио, фото), полученные от ПМС.

А.114.3.6 В верхней панели страницы «Файлы» нажать на ссылку «Рабочий каталог». Откроется корневой каталог с каталогами в файловом хранилище.

А.114.3.7 В рабочей области страницы «Файлы» выбрать каталог «reports». На странице отобразятся отчетные файлы, полученные от ПМС.

А.114.3.8 В верхней панели страницы «Файлы» нажать на ссылку «Рабочий каталог». Откроется корневой каталог с каталогами в файловом хранилище.

А.114.3.9 В рабочей области страницы «Файлы» выбрать каталог «pks». На странице отобразятся отчетные файлы, полученные от подсистемы ПКС.

А.114.3.10 В верхней части страницы в панели навигации нажать на «Настройки». Открывается страница с настройками файлового хранилища.

А.114.3.11 Выполнить настройку параметров хранения данных, установив в поля:

- «Сроки хранения данных»:
  - «Хранение информации из социальных сетей» – 1 месяц;
  - «Хранение информации из СМИ» – 2 месяца;
- «Сроки хранения файлов»:
  - «Хранение метаданных о сессиях пользователей» – 2 недели;
  - «Хранение файлов из сессии пользователей» – 2 месяца;
- «Объем хранения данных» – минимальное 16 Гб.

А.114.3.12 Выполнить настройку хранения данных, установив в поле «Выбор хранимой информации» флаги:

- данные из социальных сетей;
- файлы из социальных сетей;
- данные из интернет СМИ и веб-сайтов;
- файлы из интернет СМИ и веб-сайтов;
- отчетные файлы ПМС;
- отчетные файлы ПКС.

А.114.3.13 Нажать на кнопку «Сохранить».

А.114.4 СПО ПХД считается выдержавшим испытания по п. А.114.3.1-А.114.3.13 программы и методики испытаний и выполняющим пункты 3.2.9, 3.2.9.1 ТЗ на СЧ ОКР, если:

- на странице публикаций отобразились хранимые публикации, полученные от ПМС, с указанными настройками;
- на странице файлов отобразились файлы, полученные от ПМС, с указанными настройками;
- на странице файлов отобразились отчетные файлы, полученные от ПКС, с указанными настройками;
- сохранение настроек произошло без ошибок.

А.115 Методика № 115

А.115.1 В данной методике проводится проверка СПО ПХД на соответствие требованиям пунктов 3.2.9, 3.2.9.2 ТЗ на СЧ ОКР «Амезит-В».

А.115.2 В соответствии с требованиями пунктов 3.2.9, 3.2.9.2 ТЗ на СЧ ОКР «Амезит-В» СПО ПХД должно обеспечивать хранение шаблонов обработки новостных информационных порталов.

А.115.3 Для проведения проверки СПО ПХД на соответствие предъявляемым требованиям необходимо выполнить действия, описанные ниже.

А.115.3.1 Повторить пункты с А.114.3.1 по А.114.3.3 (Методика № 114).

А.115.3.2 В верхней части рабочей области страницы «БД» нажать на вкладку «Источники и шаблоны». Откроется страница со списком источников, с которых собирались публикации.

А.115.3.3 Возле источника нажать на значок «Шаблоны» для перехода на страницу шаблонов источника.

А.115.4 СПО ПХД считается выдержавшим испытания по п. А.115.3.1-А.115.3.3 программы и методики испытаний и выполняющим пункты 3.2.9, 3.2.9.2 ТЗ на СЧ ОКР, если в списке шаблонов выбранного источника отобразились шаблоны, используемые при сборе информации.

А.116 Методика № 116

А.116.1 В данной методике проводится проверка СПО ПХД на соответствие требованиям пунктов 3.2.9, 3.2.9.3 ТЗ на СЧ ОКР «Амезит-В».

А.116.2 В соответствии с требованиями пунктов 3.2.9, 3.2.9.3 ТЗ на СЧ ОКР «Амезит-В» СПО ПХД должно обеспечивать хранение аналитических справок, подготовленных в АПК «Амезит».

А.116.3 Для проведения проверки СПО ПХД на соответствие предъявляемым требованиям необходимо выполнить действия, описанные ниже.

А.116.3.1 Повторить пункты с А.114.3.1 по А.114.3.3 (Методика № 114).

А.116.3.2 В верхней части страницы в панели навигации нажать на «Файлы». Открывается страница с каталогами в файловом хранилище.

А.116.3.3 В рабочей области страницы «Файлы» выбрать каталог «reports». На странице отобразятся хранящиеся в подсистеме аналитические справки.

А.116.4 СПО ПХД считается выдержавшим испытания по п. А.116.3.1-А.116.3.3 программы и методики испытаний и выполняющим пункты 3.2.9, 3.2.9.3 ТЗ на СЧ ОКР, если в каталоге «reports» отобразились хранящиеся в подсистеме аналитические справки.

A.117 Методика № 117

А.117.1 В данной методике проводится проверка СПО ПХД на соответствие требованиям пунктов 3.2.9, 3.2.9.4 ТЗ на СЧ ОКР «Амезит-В».

А.117.2 В соответствии с требованиями пунктов 3.2.9, 3.2.9.4 ТЗ на СЧ ОКР «Амезит-В» СПО ПХД должно обеспечивать структурирование информации.

А.117.3 Для проведения проверки СПО ПХД на соответствие предъявляемым требованиям необходимо выполнить действия, описанные ниже.

А.117.3.1 На рабочем столе АРМ администратора запустить обозреватель.

А.117.3.2 В адресной строке ввести адрес сервиса мониторинга Kibana хранилища данных ElasticSearch и нажать на клавишу «Enter». Адрес сервера мониторинга Kibana уточняется после установки и настройки СПО ПХД согласно документу RU.BATC.00185-01 32 01 «Специальное программное обеспечение подсистемы хранения данных. Руководство системного программиста». Откроется страница сервиса мониторинга Kibana.

А.117.3.3 В правой части панели нажать на вкладку «Dev Tools». Откроется страница с полем «Console» для ввода запросов к БД на поиск данных.

А.117.3.4 В поле ввода запросов ввести запрос вида:

```
GET <имя БД>/_mappings
```

где <имя БД> − имя кластера, развернутого в БД ElasticSearch, используемого подсистемой ПМС для хранения данных. Имя индекса уточняется после установки и настройки СПО ПХД согласно документу RU.BATC.00185-01 32 01 «Специальное программное обеспечение подсистемы хранения данных. Руководство системного программиста». В окне вывода информации отобразятся все структуры данных, хранящихся в БД ElasticSearch.

А.117.3.5 На рабочем столе АРМ администратора войти в терминал, нажав левой кнопкой мыши на значок терминала. Откроется консоль.

А.117.3.6 В консоли ввести команду:

```
$  ssh root@<IP-адрес узла СУБД>
```

где <IP-адрес узла СУБД> − IP-адрес узла СУБД, на котором развернута СУБД PostgreSQL, и нажать на клавишу «Enter». IP-адрес узла БД уточняется после установки и настройки СПО ПХД согласно документу RU.BATC.00185-01 32 01 «Специальное программное обеспечение подсистемы

хранения данных. Руководство системного программиста». Будет предложено ввести пароль от пользователя root.

А.117.3.7 Ввести пароль от пользователя root (по умолчанию root). Нажать на клавишу «Enter». Будет произведено удаленное подключение к узлу СУБД.

А.117.3.8 В консоли ввести команду:

```
$  psql –h localhost –U postgres <имя бд>
```

где <имя бд> – имя БД СУБД PostgreSQL, в котором хранится сервисная информация для работы подсистемы ПМС. Имя БД уточняется после установки и настройки СПО ПХД согласно документу RU.ВАТС.00185-01 32 01 «Специальное программное обеспечение подсистемы хранения данных. Руководство системного программиста».

Будет произведен вход в консоль СУБД PostgreSQL.

А.117.3.9 В консоли ввести команду:

```
\d+ *.*
```

и нажать на клавишу «Enter». Будут отображены все структуры данных, хранящихся в БД PostgreSQL.

А.117.4 СПО ПХД считается выдержавшим испытания по п. А.117.3.1-А.117.3.9 программы и методики испытаний и выполняющим пункты 3.2.9, 3.2.9.4 ТЗ на СЧ ОКР, если:

- отобразились структуры данных, хранящихся в БД ElasticSearch;
- отобразились структуры данных, хранящихся в БД PostgreSQL.

А.118 Методика № 118

А.118.1 В данной методике проводится проверка СПО ПХД на соответствие требованиям пунктов 3.2.9, 3.2.9.5 ТЗ на СЧ ОКР «Амезит-В».

А.118.2 В соответствии с требованиями пунктов 3.2.9, 3.2.9.5 ТЗ на СЧ ОКР «Амезит-В» СПО ПХД должно обеспечивать поиск данных в массивах информации.

А.118.3 Для проведения проверки СПО ПХД на соответствие предъявляемым требованиям необходимо выполнить действия, описанные ниже.

А.118.3.1 Повторить пункты с А.114.3.1 по А.114.3.3 (Методика № 114).

А.118.3.2 На странице публикаций нажать на панель «Фильтр». Откроется панель фильтрации.

А.118.3.3 На панели фильтров заполнить поля для фильтрации на странице «Публикации»:

- в поле «Поиск» указать запрос на поиск публикаций;

- в поле «Тематики» указать тематику, по которой отбираются публикации;
- в поле «Ресурс» указать источник публикации;
- в поле «Автор» указать автора публикаций;
- в поле «Регион» указать географический регион публикации;
- в поле «Эмоциональная окраска» указать диапазон тональности публикаций;
- в поле «Дата» указать диапазон появления публикаций.

После ввода данных в поля для фильтрации на странице «Публикации» автоматически будет произведен поиск и обновится список публикаций.

А.118.3.4 В верхней части страницы в панели навигации нажать на «Файлы». Откроется страница с каталогами в файловом хранилище.

А.118.3.5 В верхней панели фильтрации выбирают поля для фильтрации на странице файлов:

- в поле «Тип файлов» указать тип отображаемых файлов;
- в поле «Дата» указать даты изменения файлов;
- в поле «Объем» указать объем файлов.

А.118.4 СПО ПХД считается выдержавшим испытания по п. А.118.3.1-А.118.3.5 программы и методики испытаний и выполняющим пункты 3.2.9, 3.2.9.5 ТЗ на СЧ ОКР, если:

- отобразились публикации, согласно указанным атрибутам поиска;
- отобразились файлы, согласно указанным атрибутам поиска.

А.119 Методика № 119

А.119.1 В данной методике проводится проверка СПО ПХД на соответствие требованиям пунктов 3.2.9, 3.2.9.6 ТЗ на СЧ ОКР «Амезит-В».

А.119.2 В соответствии с требованиями пунктов 3.2.9, 3.2.9.6 ТЗ на СЧ ОКР «Амезит-В» СПО ПХД должно обеспечивать предоставление оператору информации в графическом виде.

А.119.3 Для проведения проверки СПО ПХД на соответствие предъявляемым требованиям необходимо выполнить действия, описанные ниже.

А.119.3.1 Повторить пункты с А.114.3.1 по А.114.3.3 (Методика № 114).

А.119.3.2 На верхней панели страницы выбрать вкладку «Авторы». Откроется страница со списком авторов публикаций.

А.119.3.3 На верхней панели страницы выбрать вкладку «Источники и шаблоны». Откроется страница со списком источников публикаций.

А.119.3.4 Возле источника нажать на значок «Шаблоны» для перехода на страницу шаблонов источника.

А.119.3.5 В верхней части страницы в панели навигации нажать на «Файлы». Откроется страница с каталогами в файловом хранилище.

А.119.3.6 В верхней панели страницы выбрать вкладку «Настройки». Откроется страница с настройками файлового хранилища.

А.119.3.7 В верхней части страницы в панели навигации нажать на «Настройки». Открывается страница с настройками файлового хранилища.

А.119.4 СПО ПХД считается выдержавшим испытания по п. А.119.3.1-А.119.3.7 программы и методики испытаний и выполняющим пункты 3.2.9, 3.2.9.6 ТЗ на СЧ ОКР, если:

- отобразилась страница публикаций;
- отобразилась страница авторов публикаций;
- отобразилась страница источников публикаций;
- отобразилась страница шаблонов источников публикаций;
- отобразилась страница файлов;
- отобразилась страница настроек.

А.120 Методика № 120

А.120.1 В данной методике проводится проверка СПО ПХД на соответствие требованиям пунктов 3.2.9, 3.2.9.7 ТЗ на СЧ ОКР «Амезит-В».

А.120.2 В соответствии с требованиями пунктов 3.2.9, 3.2.9.7 ТЗ на СЧ ОКР «Амезит-В» СПО ПХД должно обеспечивать резервное копирование данных.

А.120.3 Для проведения проверки СПО ПХД на соответствие предъявляемым требованиям необходимо выполнить действия, описанные ниже.

А.120.3.1 Повторить пункты с А.114.3.1 по А.114.3.3 (Методика № 114).

А.120.3.2 В верхней части страницы в панели навигации нажать на «Настройки». Открывается страница с настройками файлового хранилища.

А.120.3.3 В поле «Сроки проведения резервного копирования» указать периодичность проведения резервного копирования.

А.120.3.4 В верхней части страницы в панели навигации нажать на «Файлы». Откроется страница с каталогами в файловом хранилище.

А.120.3.5 Произвести двойное нажатие левой кнопкой мыши на каталог «backup». Откроется страница со списком файлов − резервных копий системы.

А.120.3.6 Выполнить процедуру восстановления данных из последних резервных копий согласно документу RU.ВАТС.00185-01 46 01 «Специальное

программное обеспечение подсистемы хранения данных. Руководство по техническому обслуживанию».

А.120.4 СПО ПХД считается выдержавшим испытания по п. А.120.3.1-А.120.3.6 программы и методики испытаний и выполняющим пункты 3.2.9, 3.2.9.7 ТЗ на СЧ ОКР, если:

- резервные копии успешно создаются, согласно настроенным параметрам;
- процедура восстановления из резервных копий прошла успешно.

А.121 Методика № 121

А.121.1 В данной методике проводится проверка СПО ПХД на соответствие требованиям пунктов 3.2.9, 3.2.9.8 ТЗ на СЧ ОКР «Амезит-В».

А.121.2 В соответствии с требованиями пунктов 3.2.9, 3.2.9.8 ТЗ на СЧ ОКР «Амезит-В» СПО ПХД должно обеспечивать хранение видео-, аудиоархивов.

А.121.3 Для проведения проверки СПО ПХД на соответствие предъявляемым требованиям необходимо выполнить действия, описанные ниже.

А.121.3.1 Повторить пункты с А.114.3.1 по А.114.3.3 (Методика № 114).

А.121.3.2 В верхней части страницы в панели навигации нажать на «Файлы». Откроется страница с каталогами в файловом хранилище.

А.121.3.3 В верхней панели фильтрации выбрать поля для фильтрации на странице файлов:

- в поле «Тип файлов» указать тип файлов:
  - «Аудио» – MP3 для отображения аудиофайлов в формате mp3;
  - «Видео» – MP4 для отображения аудиофайлов в формате mp4.

А.121.4 СПО ПХД считается выдержавшим испытания по п. А.121.3.1-А.121.3.3 программы и методики испытаний и выполняющим пункты 3.2.9, 3.2.9.8 ТЗ на СЧ ОКР, если:

- в списке файлов отобразились аудиофайлы;
- в списке файлов отобразились видеофайлы;

А.122 Методика № 122

А.122.1 В данной методике проводится проверка СПО ПХД на соответствие требованиям пунктов 3.2.9, 3.2.9.9 ТЗ на СЧ ОКР «Амезит-В».

А.122.2 В соответствии с требованиями пунктов 3.2.9, 3.2.9.9 ТЗ на СЧ ОКР «Амезит-В» СПО ПХД должно обеспечивать одновременный просмотр архивов (до 3 подключений) без остановки записи.

A.122.3 Для проведения проверки СПО ПХД на соответствие предъявляемым требованиям необходимо выполнить действия, описанные ниже.

A.122.3.1 Выполнить вход в АРМ оператора 1.

A.122.3.2 На рабочем столе АРМ оператора 1 запустить проводник.

A.122.3.3 В проводнике перейти в сетевой каталог файлового хранилища. Адрес сетевого каталога уточняется после установки и настройки СПО ПХД согласно документу RU.BATC.00185-01 32 01 «Специальное программное обеспечение подсистемы хранения данных. Руководство системного программиста».

A.122.3.4 В сетевом каталоге файлового хранилища открыть каталог «media», содержащий аудио- и видеофайлы.

A.122.3.5 Сохранить аудио- или видеофайл в текущий каталог.

A.122.3.6 Не дожидаясь окончания процедуры сохранения, открыть другой видео- или аудиофайл для просмотра или прослушивания.

A.122.3.7 Выполнить вход в АРМ оператора 2.

A.122.3.8 На рабочем столе АРМ оператора 2 запустить проводник.

A.122.3.9 В проводнике перейти в сетевой каталог файлового хранилища. Адрес сетевого каталога уточняется после установки и настройки СПО ПХД согласно документу RU.BATC.00185-01 32 01 «Специальное программное обеспечение подсистемы хранения данных. Руководство системного программиста».

A.122.3.10 В сетевом каталоге файлового хранилища открыть каталог «media», содержащий аудио- и видеофайлы.

A.122.3.11 Открыть видео- или аудиофайл для просмотра или прослушивания.

A.122.3.12 Открыть видео- или аудиофайл, доступный для просмотра или прослушивания.

A.122.3.13 Выполнить вход в АРМ оператора 3.

A.122.3.14 На рабочем столе АРМ оператора 3 запустить проводник.

A.122.3.15 В проводнике перейти в сетевой каталог файлового хранилища. Адрес сетевого каталога уточняется после установки и настройки СПО ПХД согласно документу RU.BATC.00185-01 32 01 «Специальное программное обеспечение подсистемы хранения данных. Руководство системного программиста».

A.122.3.16 В сетевом каталоге файлового хранилища открыть каталог «media», содержащий аудио- и видеофайлы.

A.122.3.17 Открыть видео- или аудиофайл, доступный для просмотра или прослушивания.

A.122.4 СПО ПХД считается выдержавшим испытания по п. А.122.3.1-А.122.3.17 программы и методики испытаний и выполняющим пункты 3.2.9, 3.2.9.9 ТЗ на СЧ ОКР, если:

- при просмотре видеофайла или прослушивании аудиофайла процедура сохранения файла не была отменена;
- сохраненный оператором 1 видео- или аудиофайл доступен для просмотра или прослушивания оператору 2 и оператору 3;
- просмотр видео- или прослушивание аудиофайла доступно одновременно для оператора 1, оператора 2 и оператора 3.

A.123 Методика № 123

A.123.1 В данной методике проводится проверка СПО ПХД на соответствие требованиям пунктов 3.2.9, 3.2.9.14 ТЗ на СЧ ОКР «Амезит-В».

A.123.2 В соответствии с требованиями пунктов 3.2.9, 3.2.9.14 ТЗ на СЧ ОКР «Амезит-В» СПО ПХД должно обеспечивать автоматизированное взаимодействие с СПО подсистемы лингвистического обеспечения.

A.123.3 Для проведения проверки СПО ПХД на соответствие предъявляемым требованиям необходимо выполнить действия, описанные ниже.

A.123.3.1 Повторить пункты с А.114.3.1 по А.114.3.3 (Методика № 114).

A.123.3.2 В верхней части страницы в панели навигации нажать на «Перевод». Откроется окно перевода текста.

A.123.3.3 В поле «Текст» ввести текст для перевода.

A.123.3.4 Под полем «Текст» в выпадающем списке выбрать язык текста.

A.123.3.5 Под полем «Перевод» в выпадающем списке выбрать язык перевода.

A.123.3.6 Нажать на кнопку «Перевод». В поле «Перевод» отобразится переведенный текст.

A.123.4 СПО ПХД считается выдержавшим испытания по п. А.123.3.1-А.123.3.6 программы и методики испытаний и выполняющим пункты 3.2.9, 3.2.9.10 ТЗ на СЧ ОКР, если:

- текст был переведен;
- в процессе перевода не возникло ошибок.

A.124 Методика № 124

A.124.1 В данной методике проводится проверка СПО ПОР на соответствие требованиям пунктов 3.2.9, 3.2.9.13 ТЗ на СЧ ОКР «Амезит-В».

А.124.2 В соответствии с требованиями пунктов 3.2.9, 3.2.9.13 ТЗ на СЧ ОКР «Амезит-В» в подсистемах АПК «Амезит» обработка сведений, составляющих государственную тайну, не предусматривается, за исключением отдельного контура подсистемы ПОР, представленного обособленной группой серверов и АРМ. В указанном контуре обрабатываются сведения с грифом до «совершенно секретно» включительно.

Безопасность информации в данном контуре подсистемы ПОР должна обеспечиваться с применением сертифицированных средств защиты, отвечающих требованиям соответствующих руководящих документов.

Обеспечение доступа к обрабатываемой информации должен быть реализован путем применения межсетевого экрана, сертифицированного по требованиям 2 класса защиты в соответствии с Приказом ФСТЭК России от 9 февраля 2016 г. №9.

Обеспечение ролевого (мандатного) разграничения доступа к обрабатываемой информации должно быть реализовано на уровне операционной системы.

Доступ к информации подсистемы ПОР должен предоставляться с учетом категории пользователей и уровня полномочий, которыми наделяется каждая категория.

А.124.3 Для проведения проверки СПО ПОР ЗС на соответствие предъявляемым требованиям необходимо выполнить действия, описанные ниже.

А.124.3.1 На АРМ обработки убедиться в наличии установленного ПО «Kaspersky Anti-Virus».

А.124.3.2 На АРМ оператора ПОР ЗС выполнить вход в операционную систему Astra Linux SE 1.5 под учетной записью администратора АПК оперативного управления с уровнем доступа 2.

А.124.3.3 Выполнить вход в СПО ПОР ЗС под учетной записью администратора АПК оперативного управления.

А.124.3.4 Перейти в раздел «Администрирование», выбрать в меню пункт «Управление пользователями».

А.124.3.5 Создать учетные записи для пользователей следующих категорий: оперативный дежурный, начальник центра, оператор, администратор АПК.

А.124.3.6 В разделе «Администрирование», выбрать в меню пункт «Матрица прав», сравнить уровни полномочий, которыми наделяется каждая категория пользователей.

А.124.3.7 На АРМ оператора ПОР ЗС выполнить вход в операционную систему Astra Linux SE 1.5 под учетной записью оперативного дежурного оперативного управления с уровнем доступа 2.

А.124.3.8 Выполнить вход в СПО ПОР ЗС под учетной записью оперативный дежурный оперативного управления. Проверить текущий уровень доступа в СПО ПОР ЗС, наведя курсор на индикатор текущего уровня доступа, отображаемый в правом верхнем углу интерфейса СПО ПОР ЗС.

А.124.3.9 Перейти в модуль планирования и контроля мероприятий ЗС.

А.124.3.10 В модуле планирования и контроля мероприятий ЗС перейти поочередно в следующие разделы: «Операции», «Мероприятия», «Задачи», «Подзадачи» и «Чат».

А.124.3.11 Выполнить вход в операционную систему Astra Linux SE 1.5 под учетной записью с уровнем доступа 1.

А.124.3.12 На АРМ оператора ПОР ЗС выполнить вход в СПО ПОР ЗС под учетной записью оперативного дежурного оперативного управления. Проверить текущий уровень доступа в СПО ПОР ЗС, наведя курсор на индикатор текущего уровня доступа, отображаемый в правом верхнем углу интерфейса СПО ПОР ЗС. Убедиться в отсутствии доступа к данным разделов: «Операции», «Мероприятия», «Задачи», «Подзадачи» и «Чат».

А.124.3.13 Выполнить вход в операционную систему Astra Linux SE 1.5 под учетной записью с уровнем доступа 0.

А.124.3.14 На АРМ оператора ПОР ЗС выполнить вход в СПО ПОР ЗС под учетной записью оперативного дежурного оперативного управления. Проверить текущий уровень доступа в СПО ПОР ЗС, наведя курсор на индикатор текущего уровня доступа, отображаемый в правом верхнем углу интерфейса СПО ПОР ЗС. Убедиться в отсутствии доступа к данным разделов: «Операции», «Мероприятия», «Задачи», «Подзадачи» и «Чат».

А.124.3.15 На АРМ администратора ЗС запустить СПО ПОР ЗС и проверить разграничение доступа к информации, составляющей государственную тайну, с учетом категории пользователей и уровня полномочий, которыми наделяется каждая категория.

А.124.4 СПО ПОР считается выдержавшим испытания по п. А.124.3.1-А.124.3.15 программы и методики испытаний и выполняющим пункты 3.2.9, 3.2.9.13 на СЧ ОКР, если:

- в составе подсистемы присутствует однонаправленный шлюз «СТРОМ-1000»;
- в составе подсистемы присутствует аппаратно-программные модули доверенной загрузки «Соболь»;

- в составе присутствует ПО «Kaspersky Anti-Virus»;
- пользователям определен доступ согласно матрице доступа к информации (составляющей государственную тайну) о текущих задачах;
- отображается значение «2» индикатора текущего уровня доступа и открыт доступ к разделам интерфейса СПО ПОР ЗС при работе с уровнем доступа 2 и отсутствует доступ к разделам интерфейса СПО ПОР ЗС при работе с уровнем доступа 0 и 1.
- администратору АПК доступ к обрабатываемой информации, составляющей государственную тайну, не предоставляется.

А.125 Методика № 125

А.125.1 В данной методике проводится проверка СПО ПОР на соответствие требованиям пунктов 3.2.10, 3.2.10.1 ТЗ на СЧ ОКР «Амезит-В».

А.125.2 В соответствии с требованиями пунктов 3.2.10, 3.2.10.1 ТЗ на СЧ ОКР «Амезит-В» СПО ПОР должно обеспечивать отображение на электронной карте местности закрытого сегмента подсистемы ПОР интегрированной обстановки в геоинформационной системе с возможностью вывода цифрового формуляра объекта с графическими и текстовыми документами.

А.125.3 Для проведения проверки СПО ПОР на соответствие предъявляемым требованиям необходимо выполнить действия, описанные ниже.

А.125.3.1 На АРМ оператора ПОР ЗС запустить ГИС Оператор SE.

А.125.3.2 В ГИС Оператор SE открыть электронную карту местности.

А.125.3.3 Открыть редактор классификатора и добавить новый слой.

А.125.3.4 В классификаторе создать новый векторный объект.

А.125.3.5 На вкладке «Семантика» редактора классификатора создать следующие семантики: «Наименование», «Местонахождение», «Дополнительное описание», «Изображение» и «Формуляр».

А.125.3.6 Добавить семантики «Наименование», «Местонахождение», «Дополнительное описание», «Изображение» и «Формуляр» в список семантик объекта.

А.125.3.7 Нанести объект из ранее созданного слоя в область карты.

А.125.3.8 На карте выбрать добавленный объект. Откроется окно со свойствами объекта и семантическими характеристиками. В данном окне заполнить поле «Значение»:
- к семантической характеристике «Изображение» добавить ссылку на изображение;

- к семантической характеристике «Формуляр» добавить ссылку на документ.

A.125.3.9 Сохранить внесенные изменения.

A.125.3.10 На карте повторно выбрать добавленный объект. Откроется окно с заполненными семантическими характеристиками.

A.125.3.11 Просмотреть изображение объекта и прикрепленный текстовый документ, выбрав значение соответствующей семантической характеристики.

A.125.4 СПО ПОР считается выдержавшим испытания по п. А.125.3.1-А.125.3.11 программы и методики испытаний и выполняющим пункты 3.2.10, 3.2.10.1 ТЗ на СЧ ОКР, если:

- при выполнении вышеуказанных действий данной методики отсутствовали сообщения об ошибках;
- при активации условного знака объекта отобразился его формуляр с графическими и текстовыми документами.

A.126 Методика № 126

A.126.1 В данной методике проводится проверка СПО ПОР на соответствие требованиям пунктов 3.2.10, 3.2.10.2 ТЗ на СЧ ОКР «Амезит-В».

A.126.2 В соответствии с требованиями пунктов 3.2.10, 3.2.10.2 ТЗ на СЧ ОКР «Амезит-В» СПО ПОР должно обеспечивать отображение и редактирование (при наличии прав доступа) на электронной карте местности геоинформационной системы закрытого сегмента подсистемы ПОР формуляра (наименование, местонахождение, дополнительное описание и т.д.) при активации условного знака объекта.

A.126.3 Для проведения проверки СПО ПОР на соответствие предъявляемым требованиям необходимо выполнить действия, описанные ниже.

A.126.3.1 На АРМ оператора ПОР ЗС запустить ГИС Оператор SE.

A.126.3.2 В ГИС Оператор SE открыть электронную карту местности.

A.126.3.3 На карте выбрать объект (активировать условный знак объекта).

A.126.3.4 Отредактировать значения семантических характеристик «Наименование», «Местонахождение», «Дополнительное описание» в формуляре выбранного объекта. Сохранить внесенные изменения.

A.126.3.5 Выбрать отредактированный объект. Откроется формуляр объекта с измененными значениями семантических характеристик.

А.126.3.6 Открыть программу удаленного администрирования ГИС Администратор (из состава ГИС Сервер) от имени администратора. Для выбранного объекта изменить вид защиты выбранных данных – снять флаг «Редактирование».

А.126.3.7 Выбрать отредактированный объект. Проверить отсутствие доступа к редактированию значений семантических характеристик «Наименование», «Местонахождение», «Дополнительное описание».

А.126.4 СПО ПОР считается выдержавшим испытания по п. А.126.3.1-А.126.3.7 программы и методики испытаний и выполняющим пункты 3.2.10, 3.2.10.2 ТЗ на СЧ ОКР, если:

- при выполнении вышеуказанных действий данной методики отсутствовали сообщения об ошибках;
- при активации условного знака объекта отобразился его формуляр;
- при выполнении пп. А.126.3.5 открылся формуляр объекта с измененными значениями семантических характеристик;

при выполнении пп. А.126.3.7 у оператора отсутствует доступ на редактирование значений указанных семантических характеристик.

А.127Методика № 127

А.127.1 В данной методике проводится проверка СПО ПОР на соответствие требованиям пунктов 3.2.10, 3.2.10.3 ТЗ на СЧ ОКР «Амезит-В».

А.127.2 В соответствии с требованиями пунктов 3.2.10, 3.2.10.3 ТЗ на СЧ ОКР «Амезит-В» СПО ПОР должно обеспечивать:

- нанесение интегрированной обстановки на электронную карту местности в геоинформационной системе с АРМ оператора закрытого сегмента подсистемы ПОР;
- возможность управления электронной картой местности закрытого сегмента подсистемы ПОР на экране коллективного отображения при помощи дополнительного экрана, реагирующего на прикосновения.

Примечание. Под управлением электронной картой понимаются такие действия, как перемещение карты, изменение масштаба и активация условных знаков для просмотра электронного формуляра объекта.

А.127.3 Для проведения проверки СПО ПОР на соответствие предъявляемым требованиям необходимо выполнить действия, описанные ниже.

А.127.3.1 На АРМ оператора ПОР ЗС запустить ГИС Оператор SE.

А.127.3.2 В ГИС Оператор SE открыть электронную карту местности.

А.127.3.3 Добавить на карту объекты из существующего классификатора объектов.

А.127.3.4 Запустить СПО ПОР ЗС. В модуле планирования и контроля мероприятий ЗС выполнить последовательность действий для создания тестовой подзадачи, добавить в подзадачу ссылку на карту.

А.127.3.5 Открыть модуль визуализации состояния и статистики ЗС, перейти в тестовую подзадачу и вывести электронную карту местности ПОР на экран коллективного отображения.

А.127.3.6 Выполнить перемещение и масштабирование карты с помощью дополнительного экрана, реагирующего на прикосновения.

А.127.3.7 На карте выбрать объект (активировать условный знак объекта).

А.127.4 СПО ПОР считается выдержавшим испытания по п. А.127.3.1-А.127.3.7 программы и методики испытаний и выполняющим пункты 3.2.10, 3.2.10.3 ТЗ на СЧ ОКР, если:

- при выполнении вышеуказанных действий данной методики отсутствовали сообщения об ошибках;
- при выполнении пп. А.127.3.3 было выполнено нанесение интегрированной обстановки на электронную карту местности;
- при выполнении п. А.127.3.6 было выполнено перемещение и масштабирование карты на экране коллективного пользования;

при активации условного знака объекта отобразился его формуляр.

А.128 Методика № 128

А.128.1 В данной методике проводится проверка СПО ПОР на соответствие требованиям пунктов 3.2.10, 3.2.10.4 ТЗ на СЧ ОКР «Амезит-В».

А.128.2 В соответствии с требованиями пунктов 3.2.10, 3.2.10.4 ТЗ на СЧ ОКР «Амезит-В» СПО ПОР должно обеспечивать накопление информации в ручном режиме путем создания электронных формуляров объектов на электронной карте местности закрытого сегмента подсистемы ПОР.

А.128.3 Для проведения проверки СПО ПОР на соответствие предъявляемым требованиям необходимо выполнить действия, описанные ниже.

А.128.3.1 На АРМ оператора ПОР ЗС запустить ГИС Оператор SE.

А.128.3.2 В ГИС Оператор SE открыть электронную карту местности.

А.128.3.3 Создать слой «Объекты ПМИ».

А.128.3.4 Добавить в созданный слой объекты «Объект ПМИ 1» и «Объект ПМИ 2».

А.128.3.5 Добавить на карту объект «Объект ПМИ 1».

А.128.3.6 Сохранить изменения на карте и закрыть ГИС Оператор SE.

А.128.3.7 Повторить пп. А.128.3.1–А.128.3.2.

А.128.3.8 Добавить на карту объект «Объект ПМИ 2».

А.128.3.9 Последовательно активировать условные знаки объектов «Объект ПМИ 1» и «Объект ПМИ 2».

А.128.4 СПО ПОР считается выдержавшим испытания по п. А.128.3.1-А.128.3.9 программы и методики испытаний и выполняющим пункты 3.2.10, 3.2.10.4 ТЗ на СЧ ОКР, если:

- при выполнении вышеуказанных действий данной методики отсутствовали сообщения об ошибках;
- при выполнении пп. А.128.3.3, А.128.3.8 на электронной карте местности отображаются «Объект ПМИ 1» и «Объект ПМИ 2»;
- при активации условных знаков объектов отобразились их формуляры.

А.129 Методика № 129

А.129.1 В данной методике проводится проверка СПО ПОР на соответствие требованиям пунктов 3.2.10, 3.2.10.5 ТЗ на СЧ ОКР «Амезит-В».

А.129.2 В соответствии с требованиями пунктов 3.2.10, 3.2.10.5 ТЗ на СЧ ОКР «Амезит-В» СПО ПОР должно обеспечивать нанесение оператором графической информации на электронную карту местности закрытого сегмента подсистемы ПОР в выбранный слой с использованием библиотеки условных знаков.

А.129.3 Для проведения проверки СПО ПОР на соответствие предъявляемым требованиям необходимо выполнить действия, описанные ниже.

А.129.3.1 На АРМ оператора ПОР ЗС запустить ГИС Оператор SE.

А.129.3.2 В ГИС Оператор SE открыть электронную карту местности.

А.129.3.3 Добавить в созданный ранее слой «Объекты ПМИ» (пп. А.128.3.3) объект «Объект ПМИ 3».

А.129.3.4 Добавить на карту объект «Объект ПМИ 3».

А.129.3.5 Скрыть все слои, кроме слоя «Объекты ПМИ».

А.129.3.6 Отобразить скрытые слои.

А.129.3.7 Просмотреть библиотеку условных знаков в редакторе классификатора.

А.129.4 СПО ПОР считается выдержавшим испытания по п. А.129.3.1-А.129.3.7 программы и методики испытаний и выполняющим пункты 3.2.10, 3.2.10.5 ТЗ на СЧ ОКР, если:

- при выполнении вышеуказанных действий данной методики отсутствовали сообщения об ошибках;

- при выполнении пп. А.129.3.3, А.129.3.6 был создан объект с использованием библиотеки условных знаков;
- при выполнении пп. А.129.3.5, А.129.3.6 на электронной карте местности отображались только объекты слоя «Объекты ПМИ»;
- при выполнении пп. А.129.3.7 в библиотеке условных знаков в слое «Объекты ПМИ» присутствует условный знак «Объект ПМИ 3».

А.130 Методика № 130

А.130.1 В данной методике проводится проверка СПО ПОР на соответствие требованиям пунктов 3.2.10, 3.2.10.6 ТЗ на СЧ ОКР «Амезит-В».

А.130.2 В соответствии с требованиями пунктов 3.2.10, 3.2.10.6 ТЗ на СЧ ОКР «Амезит-В» СПО ПОР должно обеспечивать экспорт в электронные документы следующих типов:
- участков электронной карты с нанесенной обстановкой в формат Bitmap;
- текстовых данных формуляров объектов;
- вложенные данные формуляров объектов карт в формат архива ZIP.

Импорт файлов с текстовыми данными, таблицами и диаграммами осуществляется прикреплением файлов к формуляру объекта.

Должен быть реализован импорт формуляров.

А.130.3 Для проведения проверки СПО ПОР на соответствие предъявляемым требованиям необходимо выполнить действия, описанные ниже.

А.130.3.1 На АРМ оператора ПОР ЗС запустить ГИС Оператор SE.

А.130.3.2 В ГИС Оператор SE открыть электронную карту местности.

А.130.3.3 Выполнить экспорт произвольного участка электронной карты местности в формат Bitmap, сохранив изображение в предварительно созданном каталоге в файле с названием «Участок карты».

А.130.3.4 Открыть файл «Участок карты» встроенным программным средством для просмотра изображений.

А.130.3.5 Выбрать на карте объект «Объект ПМИ 1».

А.130.3.6 Выбрать файл с прикрепленными текстовыми данными, выполнить экспорт текстовых данных формуляра, сохранив их в предварительно созданном каталоге в файле с названием «Текстовые данные.odf».

А.130.3.7 Открыть файл «Текстовые данные.odf» встроенным программным средством для просмотра файлов формата odf.

А.130.3.8 Выполнить экспорт данных формуляра объекта «Объект ПМИ 1» в формат ZIP, сохранив формуляр в предварительно созданном каталоге в файле с названием «Формуляр 1».

А.130.3.9 Открыть файл «Формуляр 1» встроенным программным средством для просмотра файлов формата ZIP.

А.130.3.10 Выполнить импорт файла «Формуляр» в формуляр объекта «Объект ПМИ 1».

А.130.3.11 Выполнить импорт формуляра объекта «Объект ПМИ 1».

А.130.3.12 Проверить соответствие подключения технических средств открытого сегмента к техническим средствам закрытого сегмента ПОР схеме испытательного стенда, убедиться в наличии однонаправленного шлюза, исключающего случайный экспорт и передачу формуляров из закрытого в открытый сегмент ПОР.

А.130.4 СПО ПОР считается выдержавшим испытания по п. А.130.3.1-А.130.3.12 программы и методики испытаний и выполняющим пункты 3.2.10, 3.2.10.6 ТЗ на СЧ ОКР, если:

- при выполнении вышеуказанных действий данной методики отсутствовали сообщения об ошибках;
- при выполнении пп. А.130.3.4 был выполнен просмотр экспортированного участка карты;
- при выполнении пп. А.130.3.7 был выполнен просмотр экспортированного файла с текстовыми данными;
- при выполнении пп. А.130.3.9 был выполнен просмотр экспортированного файла с формуляром объекта;
- при выполнении пп. А.130.3.10 был выполнен импорт файла в формуляр объекта;
- при выполнении пп. А.130.3.11 был выполнен импорт формуляра объекта;
- при выполнении пп. А.130.3.12 было установлено соответствие подключения технических средств открытого сегмента к техническим средствам закрытого сегмента ПОР схеме испытательного стенда через однонаправленный шлюз.

А.131 Методика № 131

А.131.1 В данной методике проводится проверка СПО ПОР на соответствие требованиям пунктов 3.2.10, 3.2.10.7 ТЗ на СЧ ОКР «Амезит-В».

А.131.2 В соответствии с требованиями пунктов 3.2.10, 3.2.10.7 ТЗ на СЧ ОКР «Амезит-В» СПО ПОР должно обеспечивать визуальное отображение

демонстрируемой информации в многооконном режиме на средствах отображения информации (информационные окна должны иметь возможность свободно позиционироваться и масштабироваться на экране коллективного пользования).

А.131.3 Для проведения проверки СПО ПОР на соответствие предъявляемым требованиям необходимо выполнить действия, описанные ниже.

А.131.3.1 На АРМ оператора ПОР ОС запустить СПО ПОР ОС и перейти в модуль планирования и контроля мероприятий ОС согласно документу RU.BATC.00211-01 92 01 «Специальное программное обеспечение подсистемы обработки результатов и их визуализации на интерактивном экране открытого сегмента. Руководство пользователя».

А.131.3.2 Уменьшить размер окна обозревателя до четверти площади экрана и переместить его в левый верхний угол экрана.

А.131.3.3 Повторить открытие страницы модуля планирования и контроля мероприятий ОС в новом окне обозревателя.

А.131.3.4 Уменьшить размер окна обозревателя до четверти площади экрана и переместить его под первое окно обозревателя.

А.131.3.5 На АРМ оператора ПОР ЗС перейти на страницу «Видеостена» модуля визуализации состояния и статистики ЗС.

А.131.3.6 На странице «Видеостена» перейти в меню «Настройки по отображению», расположенное в правом верхнем углу.

А.131.3.7 В меню «Настройки по отображению» поочередно изменить режим отображения информации на экране:

- 1-й режим (1 монитор);
- 2-й режим (2 монитора);
- 3-й режим (3 монитора).

А.131.3.8 Убедиться, что при переходе от одного режима к другому произошло изменение пропорций (масштаба) полей экрана.

А.131.4 СПО ПОР считается выдержавшим испытания по п. А.131.3.1-А.131.3.8 программы и методики испытаний и выполняющим пункты 3.2.10, 3.2.10.7 ТЗ на СЧ ОКР, если:

- при выполнении вышеуказанных действий данной методики отсутствовали сообщения об ошибках;
- осуществлено перемещение окон на средствах отображения информации;
- осуществлено масштабирование окон на средствах отображения информации.

А.132 Методика № 132

А.132.1 В данной методике проводится проверка СПО ПОР на соответствие требованиям пунктов 3.2.10, 3.2.10.8 ТЗ на СЧ ОКР «Амезит-В».

А.132.2 В соответствии с требованиями пунктов 3.2.10, 3.2.10.8 ТЗ на СЧ ОКР «Амезит-В» СПО ПОР должно обеспечивать планирование и контроль выполнения мероприятий по информационному ограничению локального района.

А.132.3 Для проведения проверки СПО ПОР на соответствие предъявляемым требованиям необходимо выполнить действия, описанные ниже.

А.132.3.1 На АРМ оператора ПОР ЗС запустить СПО ПОР ЗС.

А.132.3.2 На АРМ оператора ПОР ЗС выполнить вход в СПО ПОР ЗС под учетной записью оперативного дежурного оперативного управления, создать операцию «Операция ПМИ 1», мероприятие «Мероприятие ПМИ 1», назначить ответственным исполнителем оперативного дежурного оперативного управления, взять в работу, создать задачу «Задача ПМИ 1 в двух сегментах», назначить ответственным исполнителем начальника отдела оперативного управления, проверить статус задачи. Взять задачу «Задача ПМИ 1 ЗС» в работу.

А.132.3.3 В рамках созданной задачи «Задача ПМИ 1 в двух сегментах» создать подзадачу «Подзадача ПМИ 1 ЗС» и назначить ответственным исполнителем оператора оперативного управления.

А.132.3.4 На АРМ оператора ПОР ЗС выполнить вход в СПО ПОР ЗС под учетной записью оператора оперативного управления, взять в работу подзадачу «Подзадача ПМИ 1 ЗС», проверить статус подзадачи. Прикрепить к подзадаче текстовый файл с отчетом о выполнении подзадачи «ПОР ПМИ Текст.txt» и дополнительные аналитические материалы (изображение «ПОР ПМИ Изображение.jpg», аудиофайл «ПОР ПМИ Аудио.mp3» и видеофайл «ПОР ПМИ Видео.avi»), добавить комментарии к подзадаче.

А.132.3.5 На АРМ оператора ПОР ОС выполнить вход в СПО ПОР ОС под учетной записью оперативного дежурного оперативного управления, создать задачу «Задача ПМИ 1 для ЗС» в рамках мероприятия ЗС, введя идентификатор задачи «Задача ПМИ 1 в двух сегментах» закрытого сегмента и назначить ответственным исполнителем начальника отдела оперативного управления. Взять задачу в работу.

А.132.3.6 В рамках созданной задачи «Задача ПМИ 1 в двух сегментах» создать подзадачу «Подзадача ПМИ 1 для ОС» и назначить ответственным исполнителем оператора оперативного управления.

А.132.3.7 На АРМ оператора ПОР ОС выполнить вход в СПО ПОР ОС под учетной записью оператора оперативного управления, взять в работу подзадачу «Подзадача ПМИ 1 для ОС», прикрепить к подзадаче текстовый файл с отчетом о выполнении подзадачи «ПОР ПМИ Текст.txt» и дополнительные аналитические материалы (изображение «ПОР ПМИ Изображение ОС.jpg», аудиофайл «ПОР ПМИ Аудио ОС.mp3» и видеофайл «ПОР ПМИ Видео ОС.avi»), добавить комментарии к подзадаче.

А.132.4 СПО ПОР считается выдержавшим испытания по п. А.132.3.1-А.132.3.7 программы и методики испытаний и выполняющим пункты 3.2.10, 3.2.10.8 ТЗ на СЧ ОКР, если:

- были созданы задачи в ОС в рамках мероприятий закрытого сегмента (ЗС) из состава операций ЗС, независящие друг от друга;
- при выполнении вышеуказанных действий данной методики отсутствовали сообщения об ошибках;
- в интерфейсе модуля планирования и контроля мероприятий ЗС отобразились созданные подзадачи;
- в модуле информационного обмена и по электронной почте ответственным исполнителям пришли уведомления об изменении статуса соответствующих операций, мероприятий, задач и подзадач;
- были получены положительные результаты проведенных проверок;
- в СПО ПОР ЗС создана операция, содержащая мероприятие и задачу, в СПО ПОР ОС создана копия задачи ЗС в легендированном виде в рамках запланированного мероприятия ЗС;
- в СПО ПОР ЗС отображаются данные подзадачи, полученные из ОС.

А.133 Методика № 133

А.133.1 В данной методике проводится проверка СПО ПОР на соответствие требованиям пунктов 3.2.10, 3.2.10.9 ТЗ на СЧ ОКР «Амезит-В».

А.133.2 В соответствии с требованиями пунктов 3.2.10, 3.2.10.9 ТЗ на СЧ ОКР «Амезит-В» СПО ПОР должно обеспечивать интегрированное представление различных видов информации (текстовой, графической, аудио и видео).

А.133.3 Для проведения проверки СПО ПОР ОС на соответствие предъявляемым требованиям необходимо выполнить действия, описанные ниже.

А.133.3.1 На АРМ оператора ПОР ЗС выполнить вход в СПО ПОР ЗС. В модуле планирования и контроля мероприятий ЗС открыть подзадачу «Подзадача ПМИ 1 ЗС», созданную ранее.

А.133.3.2 Поочередно открыть прикрепленные файлы «ПОР ПМИ Текст.txt», «ПОР ПМИ Изображение.jpg», «ПОР ПМИ Аудио.mp3», «ПОР ПМИ Видео.avi».

А.133.4 СПО ПОР считается выдержавшим испытания по п. А.133.3.1-А.133.3.2 программы и методики испытаний и выполняющим пункты 3.2.10, 3.2.10.9 ТЗ на СЧ ОКР, если:

- при выполнении вышеуказанных действий данной методики отсутствовали сообщения об ошибках;
- корректно отобразилось содержимое файлов «ПОР ПМИ Текст.txt», «ПОР ПМИ Изображение.jpg», «ПОР ПМИ Аудио.mp3», «ПОР ПМИ Видео.avi».

А.134 Методика № 134

А.134.1 В данной методике проводится проверка СПО ПОР на соответствие требованиям пунктов 3.2.10, 3.2.10.11 ТЗ на СЧ ОКР «Амезит-В».

А.134.2 В соответствии с требованиями пунктов 3.2.10, 3.2.10.11 ТЗ на СЧ ОКР «Амезит-В» СПО ПОР должно обеспечивать информационный обмен вышестоящих и подчиненных органов.

Примечания:

1. Должна быть реализована функция продолжения загрузки аудио-, видеоматериалов при разрыве соединения в ходе информационного обмена территориально удаленных элементов открытого сегмента подсистемы ПОР.
2. Взаимодействие территориально удаленных элементов открытого сегмента подсистемы ПОР осуществляется с использованием подсистемы ППД.
3. Допускается установка СПО открытого сегмента подсистемы ПОР на аппаратные средства подсистемы ППД для комплексов «Амезит-ОУ» и «Амезит-М».
4. В целях организации взаимодействия с мобильными группами, не входящими в состав АПК «Амезит», реализовать функцию подготовки временных ящиков электронной почты (Yandex, Mail.ru, Gmail), получения, отправки и удаления почтовых сообщений.

А.134.3 Для проведения проверки СПО ПОР на соответствие предъявляемым требованиям необходимо выполнить действия, описанные ниже.

А.134.3.1 На АРМ оператора ПОР ОС и сервере приложений ОС запустить СПО ПОР ОС.

А.134.3.2 В рамках созданной задачи «Задача ПМИ 1 ОС» создать подзадачу «Подзадача ПМИ 2 ОС» и назначить ответственным исполнителем оператора оперативного управления, проверить статус подзадачи.

А.134.3.3 На АРМ оператора ПОР ОС выполнить вход в СПО ПОР ОС под учетной записью оператора оперативного управления, взять в работу подзадачу «Подзадача ПМИ 2 ОС», проверить статус подзадачи. Прикрепить к подзадаче текстовый файл с отчетом о выполнении подзадачи «ПОР ПМИ Текст.txt» и дополнительные аналитические материалы (изображение «ПОР ПМИ Изображение.jpg», аудиофайл «ПОР ПМИ Аудио.mp3» и видеофайл «ПОР ПМИ Видео.avi»), добавить комментарии к подзадаче.

А.134.3.4 Во время загрузки аналитических материалов отсоединить кабель от сетевого интерфейса сервера приложений ОС. На сервере приложений ОС выполнить в терминале команду вычисления контрольной суммы md5 имени пользователя, осуществляющего загрузку: echo –n “имя пользователя” | md5sum. Перейти в каталог размещения ПОР, далее в каталог uploaddir. Убедиться в наличии директории с именем, соответствующим вычисленной контрольное сумме md5. После того как процесс загрузки будет прерван, необходимо восстановить подключение по сети, подключив кабель к сетевому интерфейсу для продолжения загрузки. Дождаться окончания загрузки.

А.134.3.5 На АРМ оператора ПОР ОС запустить клиент электронной почты Mozilla Thunderbird с настроенной учетной записью пользователя с ролью оператора оперативного управления. Отправить начальнику отдела оперативного управления управления тестовое сообщение с прикрепленным текстовым файлом «ПОР ПМИ Текст.txt».

А.134.3.6 В модуле планирования и контроля ОС в разделе «Администрирование» выбрать пункт «Редактор адресной книги». Откроется вкладка «Редактор адресной книги».

А.134.3.7 Сформировать адресную книгу для пользователя с ролью оперативного дежурного оперативного управления, установив флаг для отображения пользователей с ролью оперативного дежурного регионального центра управления.

А.134.3.8 На АРМ оператора ПОР ОС выполнить вход в СПО ПОР ОС под учетной записью оперативного дежурного оперативного управления, перейти в модуль планирования и контроля мероприятий ОС, далее в модуль информационного обмена ОС (вкладка «Чат»). Отправить тестовое сообщение оперативному дежурному регионального центра управления, выбрав его из соотвествующей группы в адресной книге.

А.134.3.9 В адресной книге навести курсор на имя пользователя с ролью оперативного дежурного регионального центра управления, во всплывающем меню нажать на кнопку «Профиль пользователя». В открывавшемся окне нажать на ссылку в поле «E-mail», соответствующую адресу электронной почты оперативного дежурного регионального центра управления. В открывшемся окне создания письма клиента электронной почты Mozilla Thunderbird отправить оперативному дежурному регионального центра управления тестовое сообщение с прикрепленным текстовым файлом «ПОР ПМИ Текст.txt».

А.134.3.10 На АРМ оператора ПОР ОС выполнить вход в СПО ПОР ОС под учетной записью оперативного дежурного регионального центра управления и открыть клиент электронной почты Mozilla Thunderbird. Прочитать полученное сообщение, открыть прикрепленный текстовый файл «ПОР ПМИ Текст.txt».

А.134.3.11 На сервере приложений ОС выполнить вход в СПО ПОР ОС под учетной записью оперативного дежурного регионального центра управления. Перейти в модуль планирования и контроля мероприятий ОС, далее в модуль информационного обмена ОС (вкладка «Чат»). Отправить тестовое сообщение оперативному дежурному оперативного управления.

А.134.3.12 На АРМ оператора ПОР ОС оперативному дежурному оперативного управления дождаться получения тестового сообщения от оперативного дежурного регионального центра управления.

А.134.3.13 На АРМ оператора ПОР ОС в модуле информационного обмена ОС навести курсор на имя пользователя с ролью оперативного дежурного регионального центра управления и убедиться, что его статус – «Доступен», а значок статуса имеет зеленый цвет. Перейти в область диалога с оперативным дежурным регионального центра управления и отправить ему файл «ПОР ПМИ Текст.txt».

А.134.3.14 На сервере приложений ОС в модуле информационного обмена ОС оперативному дежурному регионального центра управления скачать полученный файл «ПОР ПМИ Текст.txt» и открыть его.

А.134.3.15 На АРМ оператора ПОР ОС проверить доступ к службам электронной почты Yandex, Mail.Ru, Gmail, последовательно набрав в адресной строке обозревателя: mail.yandex.ru, mail.ru, gmail.com.

А.134.3.16 На АРМ оператора ОС запустить СПО ПОР ОС в обозревателе Mozilla Firefox из состава операционной системы Astra Linux SE 1.5, войти под учетной записью оператора, перейти в раздел «Подготовка почтовых ящиков» СПО ПОР ОС.

А.134.3.17 В модуле планирования и контроля мероприятий СПО ПОР ОС нажать на ссылку для загрузки плагина для автозаполнения форм, сохранить и установить плагин в соответствии с документом RU.ВАТС.00211-01 32 01 «Специальное программное обеспечение подсистемы обработки результатов и их визуализации на интерактивном экране открытого сегмента. Руководство системного программиста».

А.134.3.18 Выполнить действия:

А.134.3.18.1 Выбрать почтовую службу Mail.Ru, установить количество учетных записей – 10, нажать кнопку «Запуск подготовки к регистрации».

А.134.3.18.2 дождаться окончания генерации учетных данных 10 почтовых ящиков.

А.134.3.18.3 Нажать на кнопку «Сохранить данные в файл». Открыть файл для просмотра учетных записей. Закрыть файл.

А.134.3.18.4 Выбрать одну из учетных записей и перейти к регистрации аккаунта Mail.Ru. На странице регистрации убедиться, что обязательные поля заполнены, и нажать на кнопку «Зарегистрироваться». В случае отказа в регистрации по причине совпадения имени пользователя с уже зарегистрированным пользователем повторить попытку регистрации для другой учетной записи.

А.134.3.18.5 Войти в почтовый ящик под созданной учетной записью на странице почтовой службы Mail.Ru.

А.134.3.19 Повторить указанные выше действия для почтовых служб Gmail и Yandex.

А.134.3.20 Отправить сообщение «тест» с созданного почтового ящика почтовой службы Mail.Ru на созданные почтовые ящики служб Gmail и Yandex.

А.134.3.21 Удалить полученные тестовые сообщения на созданных почтовых ящиках служб Gmail и Yandex.

А.134.3.22 Проверка взаимодействия территориально удаленных элементов открытого сегмента ПОР с использованием ППД осуществляется предоставлением схемы организации связи.

А.134.3.23 Войти в АРМ оператора ПОР ОС под учетной записью оператора ППД. Открыть с АРМ оператора ПОР ОС (выполняет роль АРМ ППД) веб-интерфейс СПО ПОР ОС, введя в адресную строку адрес сервера ПОР ОС.

А.134.4 СПО ПОР считается выдержавшим испытания по п. А.134.3.1-А.134.3.23 программы и методики испытаний и выполняющим пункты 3.2.10, 3.3.11 ТЗ на СЧ ОКР, если:

- при выполнении вышеуказанных действий данной методики отсутствовали сообщения об ошибках;
- при восстановлении сетевого соединения процесс загрузки был возобновлен автоматически;
- отправлено сообщение с прикрепленным файлом с АРМ оператора ПОР ОС на сервер приложений ОС и обратно посредством электронной почты;
- отсутствовали сообщения об ошибках, в модуле информационного обмена операторами центра управления и регионального центра управления были получены тестовые сообщения, оператором центра управления был получен файл «ПОР ПМИ Текст.txt» от оператора регионального центра управления;
- в интерфейсе СПО сгенерированы учетные записи для подготовки 10 почтовых ящиков для почтовых служб Yandex, Mail.Ru, Gmail, учетные записи выгружены в файл, при переходе на страницу регистрации почтового ящика СПО ПОР выполнено автозаполнение полей регистрации, был выполнен успешный вход в почтовый ящик под созданной учетной записью, получено сообщение «тест» с созданного почтового ящика почтовой службы Mail.Ru, сообщение «тест» успешно удалено на почтовых ящиках служб Gmail и Yandex;
- наличие схемы организации связи;
- с АРМ ППД был открыт веб-интерфейс ПОР ОС и получен запрос на ввод логина и пароля.

А.135 Методика № 135

А.135.1 В данной методике проводится проверка СПО ПОР на соответствие требованиям пунктов 3.2.10, 3.2.10.12 ТЗ на СЧ ОКР «Амезит-В».

А.135.2 В соответствии с требованиями пунктов 3.2.10, 3.2.10.12 ТЗ на СЧ ОКР «Амезит-В» СПО ПОР должно обеспечивать автоматизированное взаимодействие с СПО подсистемы лингвистического обеспечения.

А.135.3 Для проведения проверки СПО ПОР на соответствие предъявляемым требованиям необходимо выполнить действия, описанные ниже.

А.135.3.1 Администратору АПК настроить путь до сервера подсистемы лингвистического обеспечения, добавив запись в файл конфигурации ПОР ОС config_ink.php в переменную $g_plo_server. При отсутствии подключения к подсистеме лингвистического обеспечения использовать имитатор подсистемы лингвистического обеспечения, присвоив значение переменной $g_plo_server plo_server_imitator.php.

А.135.3.2 На АРМ оператора ПОР ОС открыть «Подсистема лингвистического обеспечения ОС» в левом поле ввести текст для перевода «hello test one two three». В правом окне по мере ввода текста отображается перевод.

А.135.3.3 Для просмотра формата передаваемых данных нажать ссылку «Данные с сервера».

А.135.4 Проверка считается выполненной успешно, если:

- при выполнении вышеуказанных действий данной методики отсутствовали сообщения об ошибках;
- при выполнении пп. А.135.3.2 получен текст перевода;
- при выполнении пп. А.135.3.3 отображаются форматы отправленных и полученных данных и они соответствуют принятым форматам подсистемы лингвистического обеспечения.

А.136Методика № 136

А.136.1 В данной методике проводится проверка СПО ПОР на соответствие требованиям пункта 9.6 ТЗ на СЧ ОКР «Амезит-В».

А.136.2 В соответствии с требованиями п. 9.6 ТЗ на СЧ ОКР «Амезит-В» СПО ПОР должно обеспечивать функции обнаружения и предотвращения несанкционированной активности в режиме времени, близком к реальному

А.136.3 Для проведения проверки СПО ПОР на соответствие предъявляемым требованиям необходимо выполнить действия, описанные ниже.

А.136.3.1 На АРМ оператора ПОР ОС в терминале выполнить команду для подключения по протоколу SSH к контролируемому АРМ и ввести неправильный пароль.

А.136.3.2 На контролируемом АРМ посредством системы управления событиями ИБ «Комрад» осуществить поиск попытки авторизации с неверным паролем.

А.136.3.3 В системе управления событиями ИБ «Комрад» на странице «События» выполнить просмотр диаграммы событий в реальном времени.

А.136.4 СПО ПОР считается выдержавшим испытания по п. А.136.3.1-А.136.3.3 программы и методики испытаний и выполняющим пункт 9.6 ТЗ на СЧ ОКР, если:

- при выполнении вышеуказанных действий данной методики отсутствовали сообщения об ошибках;
- зарегистрировано событие попытки авторизации с неверным паролем на контролируемом АРМ;

- в системе управления событиями ИБ «Комрад» отобразилась диаграмма событий во времени, близком к реальному.

А.137 Методика № 137

А.137.1 В данной методике проводится проверка СПО ПОР на соответствие требованиям пунктов 9.8, 9.9 ТЗ на СЧ ОКР «Амезит-В».

А.137.2 В соответствии с требованиями пунктов 9.8, 9.9 ТЗ на СЧ ОКР «Амезит-В» СПО ПОР должно обеспечивать функции инвентаризации ресурсов и мониторинга изменений инфраструктуры АПК «Амезит».

А.137.3 Для проведения проверки СПО ПОР на соответствие предъявляемым требованиям необходимо выполнить действия, описанные ниже.

А.137.3.1 На АРМ оператора ПОР ОС выполнить запуск системы управления событиями ИБ «Комрад».

А.137.3.2 В системе управления событиями ИБ «Комрад» создать иерархическую карту инвентаризации сети.

А.137.3.3 Добавить узел (контролируемый АРМ) на карту сети.

А.137.3.4 На контролируемом АРМ перейти в терминал и выполнить команду для блокировки службы ICMP.

А.137.3.5 В веб-интерфейсе системы управления событиями ИБ «Комрад» дождаться изменения значка, отображающего статус доступности узла (контролируемого АРМ).

А.137.4 СПО ПОР считается выдержавшим испытания по п. А.137.3.1-А.137.3.5 программы и методики испытаний и выполняющим пункты 9.8, 9.9 ТЗ на СЧ ОКР, если:

- при выполнении вышеуказанных действий данной методики отсутствовали сообщения об ошибках;
- при выполнении пп. А.137.3.2, А.137.3.3 создана иерархическая карта инвентаризации сети, на которой отображен узел (контролируемый АРМ);
- при выполнении пп. А.137.3.4, А.137.3.5 осуществлена визуализация мониторинга доступности технических средств в виде иерархической карты сети.

А.138 Методика № 138

А.138.1 В данной методике проводится проверка СПО ПОР на соответствие требованиям пункта 9.10 ТЗ на СЧ ОКР «Амезит-В».

А.138.2 В соответствии с требованиями пункта 9.10 ТЗ на СЧ ОКР «Амезит-В» СПО ПОР должно обеспечивать выполнение сбора и анализа

событий информационной безопасности, поступающих с контролируемых подсистем АПК «Амезит».

А.138.3 Для проведения проверки СПО ПОР на соответствие предъявляемым требованиям необходимо выполнить действия, описанные ниже.

А.138.3.1 На АРМ оператора ПОР ОС в терминале выполнить команду для подключения по протоколу SSH к контролируемому АРМ и ввести неправильный пароль.

А.138.3.2 Осуществить поиск попытки авторизации с неверным паролем на контролируемом АРМ.

А.138.4 СПО ПОР считается выдержавшим испытания по п. А.138.3.1-А.138.3.2 программы и методики испытаний и выполняющим пункт 9.10 ТЗ на СЧ ОКР, если:

- при выполнении вышеуказанных действий данной методики отсутствовали сообщения об ошибках;
- зарегистрировано событие попытки авторизации с неверным паролем на контролируемом АРМ.

А.139Методика № 139

А.139.1 В данной методике проводится проверка СПО ПОР на соответствие требованиям пункта 9.11 ТЗ на СЧ ОКР «Амезит-В».

А.139.2 В соответствии с требованиями пункта 9.11 ТЗ на СЧ ОКР «Амезит-В» СПО ПОР должно обеспечивать визуализацию полученных данных и оповещение администратора безопасности об инцидентах информационной безопасности.

А.139.3 Для проведения проверки СПО ПОР на соответствие предъявляемым требованиям необходимо выполнить действия, описанные ниже.

А.139.4 На АРМ оператора ПОР ОС создать директиву корреляции с именем «Тестовая директива» для трех попыток авторизации с неверным паролем в течение 30 секунд, поступивших от одного источника.

А.139.5 На АРМ оператора ПОР ОС в терминале выполнить команду для подключения по протоколу SSH к контролируемому АРМ и трижды ввести неверный пароль для пользователя root.

А.139.6 Дождаться появления уведомления об инциденте.

А.139.7 На странице «Корреляция» в разделе «Инциденты» найти инцидент с именем «Тестовая директива» и просмотреть карточку инцидента.

А.139.8 СПО ПОР считается выдержавшим испытания по п. А.139.4-А.139.7 программы и методики испытаний и выполняющим пункт 9.11 ТЗ на СЧ ОКР, если:

- при выполнении вышеуказанных действий данной методики отсутствовали сообщения об ошибках;
- появились уведомления о новом инциденте информационной безопасности;
- запись об инциденте зафиксирована на странице «Корреляция» в разделе «Инциденты»;
- карточка инцидента содержит имя директивы «Тестовая директива» и записи о трех событиях авторизации с неверным паролем.

А.140 Методика № 140

А.140.1 В данной методике проводится проверка СПО «Амезит-В» на соответствие требованиям пунктов 3.4, 3.4.1-3.4.2 ТЗ на СЧ ОКР «Амезит-В».

А.140.2 В соответствии с требованиями пунктов 3.4, 3.4.1-3.4.2 ТЗ на СЧ ОКР «Амезит-В» должны быть выполнены требования живучести и стойкости к внешним воздействиям.

А.140.3 В ходе проверки оценивается качество CD-дисков с СПО «Амезит-В», а также условия применения покупных комплектующих АПК «Амезит».

А.140.3.1 Проверка качества CD-дисков с СПО «Амезит-В», выполняется сравнением эксплуатационных характеристик, представленных CD-дисков, с эксплуатационными характеристиками, предъявляемыми к CD-дискам (носителям) в соответствии с ГОСТ Р 7.0.2-2006.

А.140.3.2 Проверка условий применения покупных комплектующих АПК «Амезит» выполняется сравнением эксплуатационных характеристик, заявленных в технических условиях (ТУ) или другой сопроводительной документации на данные комплектующие, с эксплуатационными характеристиками, предъявляемыми к АПК «Амезит».

А.140.4 СПО «Амезит-В» считается выдержавшим испытания по п. А.140.3.1-А.140.3.2 программы и методики испытаний и выполняющим пункты 3.4, 3.4.1-3.4.2 ТЗ на СЧ ОКР, если:

– представленные CD-диски с СПО «Амезит-В» по эксплуатационным характеристикам соответствуют эксплуатационным характеристикам, предъявляемым к CD-дискам (носителям);
– покупные комплектующие изделия соответствуют условиям применения изделия. Устойчивость средств вычислительной техники (далее –

СВТ) к воздействию механических и климатических факторов подтверждены их ТУ и другой сопроводительной документацией.

А.141 Методика № 141

А.141.1 В данной методике проводится проверка СПО «Амезит-В» на соответствие требованиям пункта 3.5 ТЗ на СЧ ОКР «Амезит-В».

А.141.2 В соответствии с требованиями пунктов пункта 3.5 ТЗ на СЧ ОКР «Амезит-В» должны быть выполнены требования надежности.

А.141.3 Для проведения проверки СПО «Амезит-В» на соответствие предъявляемым требованиям необходимо выполнить действия, описанные ниже.

А.141.3.1 Выполнить установку, настройку и проверку СПО, входящего в состав СПО «Амезит-В», в соответствии с документами:

- RU.BATC.00177-01 32 01 «Специальное программное обеспечение подсистемы формирования автономного сегмента сети передачи данных. Руководство системного программиста»;
- RU.BATC.00178-01 32 01 «Специальное программное обеспечение подсистемы контроля сообщений автономного сегмента сети передачи данных. Руководство системного программиста»;
- RU.BATC.00179-01 32 01 «Специальное программное обеспечение подсистемы мониторинга сети Интернет и СМИ. Руководство системного программиста»;
- RU.BATC.00180-01 32 01 «Специальное программное обеспечение подсистемы анализа информационно-технических объектов телекоммуникационных систем. Руководство системного программиста»;
- RU.BATC.00180-01 32 02 «Специальное программное обеспечение подсистемы анализа информационно-технических объектов телекоммуникационных систем. Стенд контроля информационно-технических объектов систем жизнеобеспечения № 1. Руководство системного программиста»;
- RU.BATC.00180-01 32 03 «Специальное программное обеспечение подсистемы анализа информационно-технических объектов телекоммуникационных систем. Стенд контроля информационно-технических объектов систем жизнеобеспечения № 2. Руководство системного программиста»;
- RU.BATC.00181-01 32 01 «Специальное программное обеспечение подсистемы первичного анализа информации. Руководство системного программиста»;

– RU.BATC.00182-01 32 01 «Специальное программное обеспечение подсистемы ретрансляции данных с использованием промежуточных серверов. Руководство системного программиста»;

– RU.BATC.00183 -01 32 01 «Специальное программное обеспечение подсистемы подготовки, размещения и «раскрутки» специальных материалов. Руководство системного программиста»;

– RU.BATC.00184-01 32 01 «Специальное программное обеспечение подсистемы тестирования телекоммуникационного оборудования. Руководство системного программиста»;

– RU.BATC.00185-01 32 01 «Специальное программное обеспечение подсистемы хранения данных. Руководство системного программиста»;

– RU.BATC.00186-01 32 01 «Специальное программное обеспечение подсистемы обработки результатов и их визуализации на интерактивном экране. Руководство системного программиста».

А.141.3.2 Убедиться, что за заданный период времени не произошло потери конфигурационной информации вследствие отказов и сбоев аппаратной платформы.

А.141.4 СПО «Амезит-В» считается выдержавшим испытания по п. А.141.3.1-А.141.3.2 программы и методики испытаний и выполняющим пункт 3.5.1 ТЗ на СЧ ОКР, если обеспечивается исключение потери конфигурационной информации вследствие отказов и сбоев аппаратной платформы.

А.142 Методика № 142

А.142.1 В данной методике проводится проверка СПО «Амезит-В» на соответствие требованиям пунктов 3.6, 3.6.1-3.6.2 ТЗ на СЧ ОКР «Амезит-В».

А.142.2 В ходе проверки оценивается состав ролей пользователей СПО «Амезит-В», оценивается распределение функций между ними, а также полнота и качество программы эргономического обеспечения.

А.142.2.1 Проверка выполняется сравнением состава пользователей СПО «Амезит-В» и распределением функций между ними, описанных в эксплуатационной документации (руководство пользователя, руководство оператора, руководство системного программиста) с функциями, доступные пользователям в интерфейсе, а также оценкой полноты и качества программы эргономического обеспечения.

А.142.3 СПО «Амезит-В» считается выдержавшим испытания по п. А.142.2.1 программы и методики испытаний и выполняющим пункты 3.6, 3.6.1-3.6.2 ТЗ на СЧ ОКР, если:

– программа эргономического обеспечения составлена в соответствии с требованиями ГОСТ РВ 29.00-002-2005;

– состав ролей пользователей СПО «Амезит-В», описанных в эксплуатационных документах (руководство пользователя, руководство оператора, руководство системного программиста), а также распределение функций между ними соответствуют ролям и функциям пользователей, доступным в интерфейсе для каждого пользователя.

А.143 Методика № 143

А.143.1 В данной методике проводиться проверка СПО «Амезит-В» на соответствие требованиям пунктов 3.7, 3.7.1 на СЧ ОКР «Амезит-В».

А.143.2 Для проведения проверки СПО «Амезит-В» на соответствие предъявляемым требованиям необходимо выполнить действия, описанные ниже.

А.143.2.1 Выполнить техническое обслуживание СПО, входящего в состав СПО «Амезит-В», в соответствии с документами:

– RU.ВАТС.00177-01 46 01 «Специальное программное обеспечение подсистемы формирования автономного сегмента сети передачи данных. Руководство по техническому обслуживанию»;

– RU.ВАТС.00178-01 46 01 «Специальное программное обеспечение подсистемы контроля сообщений автономного сегмента сети передачи данных. Руководство по техническому обслуживанию»;

– RU.ВАТС.00179-01 46 01 «Специальное программное обеспечение подсистемы мониторинга сети Интернет и СМИ. Руководство по техническому обслуживанию»;

– RU.ВАТС.00180-01 46 01 «Специальное программное обеспечение подсистемы анализа информационно-технических объектов телекоммуникационных систем. Руководство по техническому обслуживанию»;

– RU.ВАТС.00180-01 46 02 «Специальное программное обеспечение подсистемы анализа информационно-технических объектов телекоммуникационных систем. Стенд контроля информационно-технических объектов систем жизнеобеспечения № 1. Руководство по техническому обслуживанию»;

– RU.ВАТС.00180-01 46 03 «Специальное программное обеспечение подсистемы анализа информационно-технических объектов телекоммуникационных систем. Стенд контроля информационно-технических

объектов систем жизнеобеспечения № 2. Руководство по техническому обслуживанию»;

– RU.ВАТС.00181-01 46 01 «Специальное программное обеспечение подсистемы первичного анализа информации Руководство по техническому обслуживанию»;

– RU.ВАТС.00182-01 46 01 «Специальное программное обеспечение подсистемы ретрансляции данных с использованием промежуточных серверов. Руководство по техническому обслуживанию»;

– RU.ВАТС.00183-01 46 01 «Специальное программное обеспечение подсистемы подготовки, размещения и «раскрутки» специальных материалов. Руководство по техническому обслуживанию»;

– RU.ВАТС.00184-01 46 01 «Специальное программное обеспечение подсистемы тестирования телекоммуникационного оборудования. Руководство по техническому обслуживанию»;

– RU.ВАТС.00185-01 46 01 «Специальное программное обеспечение подсистемы хранения данных. Руководство по техническому обслуживанию»;

– RU.ВАТС.00186-01 46 01 «Специальное программное обеспечение подсистемы обработки результатов и их визуализации на интерактивном экране. Руководство по техническому обслуживанию».

А.143.2.2 Убедиться, что при техническом обслуживании СПО сохранилась информация, обрабатываемая программными комплексами.

А.143.3 СПО «Амезит-В» считается выдержавшим испытания по п. А.143.2.1-А.143.2.2 программы и методики испытаний и выполняющим пункты 3.7, 3.7.1 ТЗ на СЧ ОКР, если АПК «Амезит» обеспечивает возможность проведения планового обслуживания технических средств с сохранением обрабатываемой программными комплексами информации.

А.144 Методика № 144

А.144.1 В данной методике проводится проверка СПО «Амезит-В» на соответствие требованиям пунктов 3.9, 3.9.1 ТЗ на СЧ ОКР «Амезит-В».

А.144.2 Проверка выполняется сравнением эксплуатационных характеристик, правил техники безопасности и противопожарных мероприятий, представленных в руководстве по эксплуатации АПК «Амезит», с правилами эксплуатации, техники безопасности и противопожарных мероприятий, описанных в документах: ГОСТ РВ 20.39.107-98, ГОСТ 12.2.007.0, ГОСТ 12.4.124, ГОСТ 12.1.018, ГОСТ 12.1.038, ГОСТ РВ 20.39.309-98.

А.144.3 СПО «Амезит-В» считается выдержавшим испытания по п. А.144.2 программы и методики испытаний и выполняющим пункты 3.9, 3,9.1

ТЗ на СЧ ОКР, если эксплуатационные характеристики, правила техники безопасности, противоправных мероприятий, представленные в руководстве по эксплуатации АПК «Амезит», соответствуют правилам эксплуатации, техники безопасности и противопожарных мероприятий, описанных в документах: ГОСТ РВ 20.39.107-98, ГОСТ 12.2.007.0, ГОСТ 12.4.124, ГОСТ 12.1.018, ГОСТ 12.1.038, ГОСТ РВ 20.39.309-98.

А.145 Методика № 145

А.145.1 В данной методике проводится проверка СПО «Амезит-В» на соответствие требованиям пунктов 3.10, 3.11, 9.3.1, 9.3.4, 9.3.5, 10 ТЗ на СЧ ОКР «Амезит-В».

А.145.2 В ходе проверки оценивается соответствие требованиям режима секретности, защиты от иностранных технических разведок (ИТР), требованиям защиты государственной тайны, требованиям по защите информации от несанкционированного доступа при выполнении СЧ ОКР «Амезит-В».

А.145.3 Для проведения проверки СПО «Амезит-В» на соответствие предъявляемым требованиям необходимо выполнить действия, описанные ниже.

А.145.3.1 Проверить наличие лицензий на право ведения работ, содержащих сведения, относящиеся к государственной тайне.

А.145.3.2 Убедится в том, что гриф всех документов, в которых совокупность сведений составляет государственную тайну и разработанных в рамках СЧ ОКР «Амезит-В», имеет степень секретности – «Секретно»; назначение, состав и возможности АПК «Амезит» – «Секретно»; сведения, раскрывающие режимы работы и способы использования АПК «Амезит» – «Секретно»; сведения по отдельным мероприятиям, не раскрывающим планы (замыслы) информационного противоборства – «Секретно».

А.145.3.3 Убедиться в том, что в составе документов на СЧ ОКР «Амезит-В» есть в Инструкции по защите от ИТР, разработанная в соответствии с требованиями ГОСТ РВ 50859-2010.

А.145.3.4 Убедиться в том, что в документе RU.BATC.00176-01 94 01 «Специальное программное обеспечение «Амезит-В». Руководство администратора безопасности» представлена следующая информация:

- степень секретности обрабатываемой и хранимой информации в комплексе - «несекретно»;
- класс защиты информации от НСД определен – 1Б;
- для обработки информации используются сертифицированные серийно выпускаемые в защищенном исполнении технические средства.

А.145.4 СПО «Амезит-В» считается выдержавшим испытания по п. А.145.3.1-А.145.3.4 программы и методики испытаний и выполняющим пункты 3.10, 3.11, 9.3.1, 9.3.4, 9.3.5, 10 ТЗ на СЧ ОКР, если полученные результаты (проверок п. А.145.3.1-А.145.3.4 программы и методики испытаний) соответствуют предъявленным требованиям в полном объеме.

А.146 Методика № 146

А.146.1 В данной методике проводится проверка СПО «Амезит-В» на соответствие требованиям пунктов 3.12, 3.12.1-3.12.4 ТЗ на СЧ ОКР «Амезит-В».

А.146.2 В соотвествии с требованиями пунктов 3.12, 3.12.1-3.12.4 ТЗ на СЧ ОКР «Амезит-В» СПО «Амезит-В» дожно быть стандартизировано, унифицировано и каталогизировано.

А.146.3 Для проведения проверки СПО «Амезит-В» на соответствие предъявляемым требованиям необходимо выполнить действия, описанные ниже.

А.146.3.1 В интерфейсе пользователя СПО «Амезит-В» выполнить формирование отчета в соответствии с документами:

- RU.BATC.00177-01 92 01 «Специальное программное обеспечение подсистемы формирования автономного сегмента сети передачи данных. Руководство пользователя»;
- RU.BATC.00178-01 92 01 «Специальное программное обеспечение подсистемы контроля сообщений автономного сегмента сети передачи данных. Руководство пользователя»;
- RU.BATC.00179-01 92 01 «Специальное программное обеспечение подсистемы мониторинга сети Интернет и СМИ. Руководство пользователя»;
- RU.BATC.00180-01 92 01 «Специальное программное обеспечение подсистемы анализа информационно-технических объектов телекоммуникационных систем. Руководство пользователя»;
- RU.BATC.00181-01 92 01 «Специальное программное обеспечение подсистемы первичного анализа информации. Руководство пользователя»;
- RU.BATC.00182-01 92 01 «Специальное программное обеспечение подсистемы ретрансляции данных с использованием промежуточных серверов. Руководство пользователя»;
- RU.BATC.00183-01 92 01 «Специальное программное обеспечение подсистемы подготовки, размещения и «раскрутки» специальных материалов. Руководство пользователя»;

– RU.BATC.00184-01 92 01 «Специальное программное обеспечение подсистемы тестирования телекоммуникационного оборудования. Руководство пользователя»;

– RU.BATC.00185-01 92 01 «Специальное программное обеспечение подсистемы хранения данных. Руководство пользователя»;

– RU.BATC.00186-01 92 01 «Специальное программное обеспечение подсистемы обработки результатов и их визуализации на интерактивном экране. Руководство пользователя».

А.146.3.2 Убедиться, что сформированные отчеты единообразно структурированы и имеют одинаковое функциональное назначение.

А.146.3.3 Выполнить запуск СПО «Амезит-В» в соответствии с документами:

– RU.BATC.00177-01 34 01 «Специальное программное обеспечение подсистемы формирования автономного сегмента сети передачи данных. Руководство оператора»;

– RU.BATC.00178-01 34 01 «Специальное программное обеспечение подсистемы контроля сообщений автономного сегмента сети передачи данных. Руководство оператора»;

– RU.BATC.00179-01 34 01 «Специальное программное обеспечение подсистемы мониторинга сети Интернет и СМИ. Руководство оператора»;

– RU.BATC.00180-01 34 01 «Специальное программное обеспечение подсистемы анализа информационно-технических объектов телекоммуникационных систем. Руководство оператора»;

– RU.BATC.00181-01 34 01 «Специальное программное обеспечение подсистемы первичного анализа информации. Руководство оператора»;

– RU.BATC.00182-01 34 01 «Специальное программное обеспечение подсистемы ретрансляции данных с использованием промежуточных серверов. Руководство оператора»;

– RU.BATC.00183-01 34 01 «Специальное программное обеспечение подсистемы подготовки, размещения и «раскрутки» специальных материалов. Руководство оператора»;

– RU.BATC.00184-01 34 01 «Специальное программное обеспечение подсистемы тестирования телекоммуникационного оборудования. Руководство оператора»;

– RU.BATC.00185-01 34 01 «Специальное программное обеспечение подсистемы хранения данных. Руководство оператора»;

– RU.BATC.00186-01 34 01 «Специальное программное обеспечение подсистемы обработки результатов и их визуализации на интерактивном экране. Руководство оператора».

А.146.3.4 Убедиться, что СПО «Амезит-В» стандартизировано и унифицировано и имеет следующие качественные показатели – СПО «Амезит» запускается через обозреватель, построено по технологии тонкий клиент (клиент-серверная архитектура), экранные формы интерфейса имеют единый стиль представления.

А.146.4 СПО «Амезит-В» считается выдержавшим испытания по п. А.146.3.1-А.146.3.4 программы и методики испытаний и выполняющим пункты 3.12, 3.12.1-3.12.4 ТЗ на СЧ ОКР, если:

– стандартизация и унификация форм документов, циркулирующих в изделии обеспечена за счет совершенствования форм и уменьшения многообразия документов одинакового функционального назначения;

– выполнены требования по стандартизации и унификации, порядок задания и состав в соответствии с ГОСТ В 15.207, ГОСТ В 20.39.105;

– в материалах технического проекта отражены сведения о существующих аналогах разрабатываемого изделия;

– СПО обеспечивает использование разрабатываемых и перспективных решений по планомерной модернизации комплекса и создание различных модификаций. При этом обеспечена максимальная унификация образцов.

А.147 Методика № 147

А.147.1 В данной методике проводится проверка СПО «Амезит-В» на соответствие требованиям пунктов 3.14, 3.14.1, 7, 7.1-7.2 ТЗ на СЧ ОКР «Амезит-В».

А.147.2 Согласно требованиям пунктов 3.14, 3.14.1, 7, 7.1-7.2 ТЗ на СЧ ОКР «Амезит-В» СПО «Амезит-В» должно выдерживать конструктивные требований, требования к консервации, упаковке и маркировке

А.147.3 Проверка выполняется путем визуального осмотра упаковки ЛКД.

А.147.4 СПО «Амезит-В» считается выдержавшим испытания по п. А.147.3 программы и методики испытаний и выполняющим пункты 3.14, 3.14.1, 7, 7.1-7.2 ТЗ на СЧ ОКР, если:

– на упаковках ЛКД нанесена маркировка содержащая манипуляционный знак, основные и информационные надписи;

– количество ЛКД в одной упаковке – 1 шт.;

– маркировка, наносимая на упаковку удовлетворяет требованиям ГОСТ РВ 20.39.309-98;

– маркировка устойчива, механически прочная, не стирается, не смывается жидкостями, используемыми при эксплуатации;

– консервация упаковки удовлетворяет требованиям ГОСТ 9.014-78, ГОСТ РВ 20.39.309-98.

А.148 Методика № 148

А.148.1 В данной методике проводится проверка СПО «Амезит-В» на соответствие требованиям пунктов 4.1-4.3 ТЗ на СЧ ОКР «Амезит-В».

А.148.2 В ходе проверки оценивается технико-экономические требования, предъявляемые к СПО «Амезит-В».

А.148.3 Оцениваются следующие показатели:

– расчет контрактной цены СЧ ОКР «Амезит-В»;

– объем выполненных работ;

– результаты технико-экономического обоснования создаваемого СПО.

А.148.4 Для проведения проверки СПО «Амезит-В» на соответствие предъявляемым требованиям необходимо выполнить действия, описанные ниже.

А.148.5 Проверить наличие утвержденного акта материально-технической приемки (МТП). Убедиться, что состав ОО и объем выполненных работ соответствует составу и объему работ, заявленных в акте МТП.

А.148.6 Проверить расчет контрактной. Убедиться, что расчет контрактной цены СЧ ОКР «Амезит-В» производился исходя из исходя из плановых затрат при выполнении объема работ, установленного ТЗ, методом прямого счета по статьям калькуляции, в соответствии с положениями:

– Постановление Правительства РФ от 13 декабря 2013 года № 1155 «Об утверждении Положения о применении видов цен на продукцию по государственному оборонному заказу»;

– Постановление Правительства РФ от 5 декабря 2013 года № 1119 «Об утверждении Положения о государственном регулировании цен на продукцию, поставляемую по государственному оборонному заказу» (в ред. Постановлений Правительства РФ от 03.12.2014 г. № 1298, от 04.09.2015 г. № 941);

– Постановление Правительства РФ от 28 апреля 2015 года № 407 «О порядке определения начальной (максимальной) цены государственного контракта, а также цены государственного контракта, заключаемого с единственным поставщиком (подрядчиком, исполнителем), при

осуществлении закупок товаров, работ, услуг по государственному оборонному заказу» (в ред. Постановления Правительства РФ от 04.09.2015 г. № 941);

– Приказа Минпромэнерго России от 23 августа 2006 года № 200 «Об утверждении Порядка определения состава затрат на производство продукции оборонного назначения поставляемой по государственному оборонному заказу» (в ред. Приказа Минпромэнерго России от 07.11.2013 г. № 1773);

– других действующих законодательных и нормативно-правовых актов Российской Федерации.

А.148.7 Убедиться, что исходными данными при определении контрактной цены СЧ ОКР являлись: ТЗ на СЧ ОКР, трудоемкость СЧ ОКР в соответствии с ТЗ на СЧ ОКР «Амезит-В», ведомость исполнения, экономические показатели по НИОКР, установленные на 2016 г. и согласованные 474 военным представительством МО РФ.

А.148.8 Убедиться, что контрактная цена СЧ КОР «Амезит-В» составляет 270 000 000,00 (Двести семьдесят миллионов) руб. 00 коп.

А.148.9 Проверить содержание итогового отчета по СЧ ОКР, убедиться, что технико-экономические обоснования создания СПО определены следующими показателями:

– ориентировочная стоимость, продолжительность подготовки и освоения серийного производства;

– ориентировочная цена СПО в серийном производстве;

– стоимость этапов жизненного цикла, в том числе предельная стоимость производства СПО, предельная среднегодовая стоимость эксплуатации изделий и содержания его в процессе хранения;

– предельная трудоемкость изготовления СПО в серийном производстве.

А.148.10 СПО «Амезит-В» считается выдержавшим испытания по п. А.148.5-А.148.9 программы и методики испытаний и выполняющим пункты 4.1-4.3 ТЗ на СЧ ОКР, если расчет контрактной цены СЧ ОКР «Амезит-В», объем выполненных работ, результаты технико-экономического обоснования создаваемого СПО, соответствуют требованиям, завяленным в пунктах 4.1-4.3 ТЗ на СЧ ОКР «Амезит-В».

А.149 Методика № 149

А.149.1 В данной методике проводится проверка СПО «Амезит-В» на соответствие требованиям пунктов 5.3, 5.3.1-5.3.4 ТЗ на СЧ ОКР «Амезит-В».

А.149.2 Согласно пункту 5.3.1 ТЗ на СЧ ОКР «Амезит-В» диагностическое обеспечение изделия должно осуществляться в соответствии с ГОСТ 26656, ГОСТ 27518 и других действующих НТД.

А.149.3 Согласно требованиям пункта 5.3.2 ТЗ на СЧ ОКР «Амезит-В» На этапе эскизного проекта уточняются и согласовываются с головным исполнителем следующие требования по диагностическому обеспечению:

- количественные значения показателей технического диагностирования; требования приспособленности к техническому диагностированию (контролепригодности) образца;
- требования к номенклатуре диагностируемых (контролируемых) параметров и их характеристик;
- требования к средствам технического диагностирования (контроля технического состояния);
- требования к методам и правилам технического диагностирования (контроля технического состояния);
- условные вероятности необнаруженного и ложного отказов (неисправностей) в изделии с точностью, до которой определяется место отказа (неисправности);
- условная вероятность ошибочного прогнозирования безопасной эксплуатации;
- периодичность и продолжительность технического диагностирования (контроля технического состояния);
- глубина поиска неисправностей и полнота технического диагностирования (контроля технического состояния).

А.149.4 Согласно требованиям пункта 5.3.3 ТЗ на СЧ ОКР «Амезит-В» обоснование требований по диагностическому обеспечению, показателей технического диагностирования, а также ограничений на эти показатели должно проводиться исходя из достижения максимально возможной эффективности применения изделия.

А.149.5 Согласно пункту 5.3.4 ТЗ на СЧ ОКР «Амезит-В» для обеспечения эксплуатационного контроля и диагностики неисправностей в разрабатываемом изделии должны быть предусмотрены программные методы обнаружения и локализации неисправностей ПО подсистем.

А.149.6 Для проверки требований пунктов 5.3.1-5.3.3 ТЗ на СЧ ОКР необходимо открыть согласованные требования по диагностическому обеспечению СПО «Амезит-В» (исх. 120/5140с ФГУП «РНИИРС» от 25.10.2017 г.). Убедиться, что:

– диагностическое обеспечение СПО «Амезит» разработано в соответствии с ГОСТ 26656, ГОСТ 27518 и другими действующими НТД;

– определены следующие показатели:

  – количественные значения показателей технического диагностирования; требования приспособленности к техническому диагностированию (контролепригодности) образца;
  – требования к номенклатуре диагностируемых (контролируемых) параметров и их характеристик;
  – требования к средствам технического диагностирования (контроля технического состояния);
  – требования к методам и правилам технического диагностирования (контроля технического состояния);
  – условные вероятности необнаруженного и ложного отказов (неисправностей) в изделии с точностью, до которой определяется место отказа (неисправности);
  – условная вероятность ошибочного прогнозирования безопасной эксплуатации;
  – периодичность и продолжительность технического диагностирования (контроля технического состояния);
  – глубина поиска неисправностей и полнота технического диагностирования (контроля технического состояния);

– обоснование требований по диагностическому обеспечению, показателей технического диагностирования, а также ограничений на эти показатели приведено исходя из достижения максимально возможной эффективности применения изделия.

А.149.7 Для проведения проверки СПО «Амезит-В» на соответствие требованиям пункта 5.3.4 ТЗ на СЧ ОКР «Амезит-В» выполнить действия, описанные ниже.

А.149.7.1 Запустить СПО «Амезит-В» в соответствии с документами:

– RU.ВАТС.00177-01 92 01 «Специальное программное обеспечение подсистемы формирования автономного сегмента сети передачи данных. Руководство пользователя»;

– RU.ВАТС.00178-01 92 01 «Специальное программное обеспечение подсистемы контроля сообщений автономного сегмента сети передачи данных. Руководство пользователя»;

– RU.BATC.00179-01 92 01 «Специальное программное обеспечение подсистемы мониторинга сети Интернет и СМИ. Руководство пользователя»;

– RU.BATC.00180-01 92 01 «Специальное программное обеспечение подсистемы анализа информационно-технических объектов телекоммуникационных систем. Руководство пользователя»;

– RU.BATC.00181-01 92 01 «Специальное программное обеспечение подсистемы первичного анализа информации. Руководство пользователя»;

– RU.BATC.00182-01 92 01 «Специальное программное обеспечение подсистемы ретрансляции данных с использованием промежуточных серверов. Руководство пользователя»;

– RU.BATC.00183-01 92 01 «Специальное программное обеспечение подсистемы подготовки, размещения и «раскрутки» специальных материалов. Руководство пользователя»;

– RU.BATC.00184-01 92 01 «Специальное программное обеспечение подсистемы тестирования телекоммуникационного оборудования. Руководство пользователя»;

– RU.BATC.00185-01 92 01 «Специальное программное обеспечение подсистемы хранения данных. Руководство пользователя»;

– RU.BATC.00186-01 92 01 «Специальное программное обеспечение подсистемы обработки результатов и их визуализации на интерактивном экране. Руководство пользователя».

А.149.7.2 Одновременно с с запуском СПО «Амезит-В» выполнить скрипт diag.sh/diag.bat. Также, возможно добавление скрипта в cron либо иной планировщик для периодического контроля.

Входными данными для скрипта является файл checksum.dat построчно содержащий следующие значения <полный путь до компонента, название подсистемы компонента, контрольная сумма в формате md5> без пробелов. Например:

D:\first.rar,testModule,cf4de6a10e4d1c6506be3867e608810c

D:\first.rar,testModule2,cf4de6a10e4d1c6506be3867e6088101.

А.149.7.3 Убедиться, что СПО «Амезит-В» контольная сумма соотвествует контрольной сумме, заявленной в эксплуатационной документации на СПО «Амезит-В».

А.149.8 СПО «Амезит-В» считается выдержавшим испытания по п. А.149.6-А.149.7.2 программы и методики испытаний и выполняющим пункты 5.3, 5.3.1-5.3.4 ТЗ на СЧ ОКР, если:

– диагностическое обеспечение СПО «Амезит» разработано в соответствии с ГОСТ 26656, ГОСТ 27518 и другими действующими НТД;

- определены следующие показатели:
- количественные значения показателей технического диагностирования; требования приспособленности к техническому диагностированию (контролепригодности) образца;
- требования к номенклатуре диагностируемых (контролируемых) параметров и их характеристик;
- требования к средствам технического диагностирования (контроля технического состояния);
- требования к методам и правилам технического диагностирования (контроля технического состояния);
- условные вероятности необнаруженного и ложного отказов (неисправностей) в изделии с точностью, до которой определяется место отказа (неисправности);
- условная вероятность ошибочного прогнозирования безопасной эксплуатации;
- периодичность и продолжительность технического диагностирования (контроля технического состояния);
- глубина поиска неисправностей и полнота технического диагностирования (контроля технического состояния);

– обоснование требований по диагностическому обеспечению, показателей технического диагностирования, а также ограничений на эти показатели приведено исходя из достижения максимально возможной эффективности применения изделия;

– для обеспечения эксплуатационного контроля и диагностики неисправностей в разрабатываемом изделии предусмотрены программные методы обнаружения и локализации неисправностей ПО подсистем.

А.150 Методика № 150

А.150.1 В данной методике проводится проверка СПО «Амезит-В» на соответствие требованиям пунктов 5.4, 5.4.1-5.4.2.1, 5.4.2.4-5.4.3.3 ТЗ на СЧ ОКР «Амезит-В».

А.150.2 В ходе проверки оценивается математическое, программному и информационно-лингвистическому обеспечению СПО «Амезит-В».

А.150.1 Для проведения проверки СПО «Амезит-В» на соответствие требованиям пунктов 5.4.1.1-5.4.1.3 необходимо выполнить действия, описанные ниже.

А.150.1.1 Выполнить анализ программной документации:

– RU.BATC.00177-01 13 01 «Специальное программное обеспечение подсистемы формирования автономного сегмента сети передачи данных. Описание программы»;

– RU.BATC.00178-01 13 01 «Специальное программное обеспечение подсистемы контроля сообщений автономного сегмента сети передачи данных. Описание программы»;

– RU.BATC.00179-01 13 01 «Специальное программное обеспечение подсистемы мониторинга сети Интернет и СМИ. Описание программы»;

– RU.BATC.00180-01 13 01 «Специальное программное обеспечение подсистемы анализа информационно-технических объектов телекоммуникационных систем. Описание программы»;

– RU.BATC.00181-01 13 01 «Специальное программное обеспечение подсистемы первичного анализа информации. Описание программы»;

– RU.BATC.00182-01 13 01 «Специальное программное обеспечение подсистемы ретрансляции данных с использованием промежуточных серверов. Описание программы»;

– RU.BATC.00183-01 13 01 «Специальное программное обеспечение подсистемы подготовки, размещения и «раскрутки» специальных материалов. Описание программы»;

– RU.BATC.00184-01 13 01 «Специальное программное обеспечение подсистемы тестирования телекоммуникационного оборудования. Описание программы»;

– RU.BATC.00185-01 13 01 «Специальное программное обеспечение подсистемы хранения данных. Описание программы»;

– RU.BATC.00186-01 13 01 «Специальное программное обеспечение подсистемы обработки результатов и их визуализации на интерактивном экране. Описание программы».

А.150.1.2 СПО «Амезит-В» считается выдержавшим испытания по п. А.150.1.1 программы и методики испытаний и выполняющим пункты 5.4.1.1-5.4.1.3 ТЗ на СЧ ОКР, если:

– программная документация содержит:
  – математические методы и алгоритмы обработки данных;
  – математические методы и алгоритмы визуального представления информации о результатах обработки данных;

– методы, модели и алгоритмы детально описаны, документированы и независимы от их программной реализации.

– модели и алгоритмы разработаны с максимальным использованием отработанных типовых моделей, методов и алгоритмов.

А.150.2 Для проведения проверки СПО «Амезит-В» на соответствие требованиям пунктов 5.4.2.1, 5.4.2.4-5.4.3.2 необходимо выполнить действия, описанные ниже.

А.150.2.1 Выполнить установку, настройку и запуск СПО «Амезит-В» в соответствии с эксплуатационной документами:

– RU.ВАТС.00177-01 32 01 «Специальное программное обеспечение подсистемы формирования автономного сегмента сети передачи данных. Руководство системного программиста»;

– RU.ВАТС.00178-01 32 01 «Специальное программное обеспечение подсистемы контроля сообщений автономного сегмента сети передачи данных. Руководство системного программиста»;

– RU.ВАТС.00179-01 32 01 «Специальное программное обеспечение подсистемы мониторинга сети Интернет и СМИ. Руководство системного программиста»;

– RU.ВАТС.00180-01 32 01 «Специальное программное обеспечение подсистемы анализа информационно-технических объектов телекоммуникационных систем. Руководство системного программиста»;

– RU.ВАТС.00181-01 32 01 «Специальное программное обеспечение подсистемы первичного анализа информации. Руководство системного программиста»;

– RU.ВАТС.00182-01 32 01 «Специальное программное обеспечение подсистемы ретрансляции данных с использованием промежуточных серверов. Руководство системного программиста»;

– RU.ВАТС.00183-01 32 01 «Специальное программное обеспечение подсистемы подготовки, размещения и «раскрутки» специальных материалов. Руководство системного программиста»;

– RU.ВАТС.00184-01 32 01 «Специальное программное обеспечение подсистемы тестирования телекоммуникационного оборудования. Руководство системного программиста»;

– RU.ВАТС.00185-01 32 01 «Специальное программное обеспечение подсистемы хранения данных. Руководство системного программиста»;

– RU.ВАТС.00186-01 32 01 «Специальное программное обеспечение подсистемы обработки результатов и их визуализации на интерактивном экране. Руководство системного программиста».

А.150.2.2 В интерфейсе пользователя выполнить необходимые операции в соответствии с эксплуатационными документами:

– RU.ВАТС.00177-01 92 01 «Специальное программное обеспечение подсистемы формирования автономного сегмента сети передачи данных. Руководство пользователя»;

– RU.ВАТС.00178-01 92 01 «Специальное программное обеспечение подсистемы контроля сообщений автономного сегмента сети передачи данных. Руководство пользователя»;

– RU.ВАТС.00179-01 92 01 «Специальное программное обеспечение подсистемы мониторинга сети Интернет и СМИ. Руководство пользователя»;

– RU.ВАТС.00180-01 92 01 «Специальное программное обеспечение подсистемы анализа информационно-технических объектов телекоммуникационных систем. Руководство пользователя»;

– RU.ВАТС.00181-01 92 01 «Специальное программное обеспечение подсистемы первичного анализа информации. Руководство пользователя»;

– RU.ВАТС.00182-01 92 01 «Специальное программное обеспечение подсистемы ретрансляции данных с использованием промежуточных серверов. Руководство пользователя»;

– RU.ВАТС.00183-01 92 01 «Специальное программное обеспечение подсистемы подготовки, размещения и «раскрутки» специальных материалов. Руководство пользователя»;

– RU.ВАТС.00184-01 92 01 «Специальное программное обеспечение подсистемы тестирования телекоммуникационного оборудования. Руководство пользователя»;

– RU.ВАТС.00185-01 92 01 «Специальное программное обеспечение подсистемы хранения данных. Руководство пользователя»;

– RU.ВАТС.00186-01 92 01 «Специальное программное обеспечение подсистемы обработки результатов и их визуализации на интерактивном экране. Руководство пользователя».

А.150.2.3 СПО «Амезит-В» считается выдержавшим испытания по п. А.150.2.1-А.150.2.2 программы и методики испытаний и выполняющим пункты 5.4.2.1, 5.4.2.4-5.4.3.2 ТЗ на СЧ ОКР, если:

– ОПО СПО «Амезит-В» инсталлировалось в минимально необходимой для работы конфигурации и не содержит в своем составе игровых программ;

– используемые операционные системы персональных ЭВМ, имеют полный набор сервисов по компоновке программных модулей, сетевому взаимодействию, включению в состав систем и исключению из их состава

различных аппаратных средств, контролю безопасности информации, отображения информации и обеспечению функционирования распределенных баз данных, независимо от того, на каких средствах вычислительной техники они работают;

– программные средства СПО «Амезит-В» поддерживают эталонную модель взаимосвязи открытых систем и обеспечивают независимость программ прикладного уровня от сетевой среды;

– программные средства, входящие в состав СПО «Амезит-В» совместимы между собой;

– программные средства, входящие в состав СПО «Амезит-В» совместимы между собой;

– интерфейс программных средств СПО «Амезит-В» обладает семантической прозрачностью, однозначностью и интуитивно понятной доступностью для различных категорий пользователей независимо от используемых средств вычислительной техники и операционной среды;

– при разработке СПО «Амезит-В» использовались средства автоматизированной отладки, поддерживающие синтаксический и семантический контроль правильности модулей, написанных на языках программирования различного уровня и языках информационных систем (систем управления базами данных, электронных таблиц и т.п.) и контроль их трансляции в машинный код команд ЭВМ. Используемые средства автоматизированной отладки обеспечивают выполнение следующих функций:

- контроль правильности исходных текстов программ и выдачу информации о месте и характере ошибок;
- выдачу результатов отладки и необходимых промежуточных данных на языке отладки после их предварительной обработки;
- возможность корректировки отлаживаемой программы с целью исправления обнаруженных ошибок.

– предусмотрена возможность расширять функциональность без существенных доработок программного кода (построение по модульному принципу);

– программные интерфейсы расширения четко документированы и входят в состав эксплуатационной документации.

– все функции СПО поддерживают русский язык и обеспечивают русскоязычный интерфейс пользователя (с учетом требований легендирования);

– СПО обеспечивает обработку информационных документов на поддерживаемых Unicode языках. При этом учитывается морфология для документов на русском и английском языках.

А.150.3 Для проведения проверки СПО «Амезит-В» на соответствие требованиям пункта 5.4.3.3 необходимо выполнить действия, описанные ниже.

А.150.3.1 Выполнить запуск СПО ПМС в соответствии с документом RU.BATC.00179-01 32 01 «Специальное программное обеспечение подсистемы мониторинга сети Интернет и СМИ. Руководство системного программиста».

А.150.3.2 Запустить ElasticSearch и выполнить в консоли следующую команду:

```
 GET amesyte/post/_search
{
  "query": {
    "match": {
      "post_text": "сирия игил"
    }
  },
  size: 100
}
```

А.150.3.3 Убедиться, что в результате выполнения команды найдены все посты, в которых употребояется слово «Сирия» или «Игил».

А.150.3.4 Запустить ElasticSearch и выполнить в консоли следующую команду:

```
GET amesyte/author/_search
{
  "query": {
    "match": {
      "name_analyzed": "Владимир"
    }
  }
}
```

А.150.3.5 Убедиться, что в результате выполнения команды найдены все авторы, полное имя которого «Владимир».

А.150.3.6 Запустить ElasticSearch и выполнить в консоли следующую команду:

```
GET amesyte/post/_search
{
  "size": 0,
  "aggs": {
    "hosts": {
      "terms": {
        "field": "url_host",
        "size": 10
      }
    }
  }
}
```

А.150.3.7 Убедиться, что в результате выполнения команды отобразились все источники, в которых были собраны публикации, с указанием количества постов по каждому источнику.

А.150.3.8 Запустить ElasticSearch и выполнить в консоли следующую команду:

```
GET amesyte/post/_search
{
  "query": {
    "query_string": {
      "default_field": "post_text",
      "query": "+(Сирия Аль-Нусра) -(США)"
    }
  }
}
```

А.150.3.9 Убедиться, что в результате выполнения команды (использования специализированного запроса) найдены все посты, в которых обязательно употреблялись слова «Сирия» или «Аль-Нусра» и не было употребление слова «США».

А.150.3.10 Запустить ElasticSearch и выполнить в консоли следующую команду:

```
GET amesyte/post/_search
{
  "query": {
    "bool": {
      "must": [
        {
          "term": {
            "rco_objects.original.keyword": {
              "value": "ЭРДОГАН"
            }
          }
        }
      ]
    }
  },
  "aggs": {
    "objects": {
      "terms": {
        "field": "rco_objects.original.keyword"
      }
    }
  }
}
```

А.150.3.11 Убедиться, что в результате выполнения команды отобразились все объекты, в публикациях которых семантическим анализатором была найдена персона «ЭРДОГАН» (регистр не учитывается).

А.150.3.12 Запустить PostgreSQL (база данных веб-интерфейса) и в консоли выполнить команду:

```
select * from login_user
```

А.150.3.13 Убедиться, что в результате выполнения команды отобразился список всех пользователей подсистемы СПО ПМС.

А.150.3.14 Запустить PostgreSQL (база данных веб-интерфейса) и в консоли выполнить команду:

```
select * from themes
```

А.150.3.15 Убедиться, что в результате выполнения команды отобразился список всех тематик всех пользователей подсистемы СПО ПМС.

А.150.3.16 Запустить PostgreSQL (база данных веб-интерфейса) и в консоли выполнить команду:

```
select * from notifications where viewed=false
```

А.150.3.17 Убедиться, что в результате выполнения команды отобразился список всех тематик всех непросмотренных уведомлений всех пользователей подсистемы СПО ПМС.

А.150.3.18 Запустить PostgreSQL (база данных сборщика СМИ) и выполнить команду:

```
select * from sources
```

А.150.3.19 Убедиться, что в результате выполнения команды отобразился список всех источника сборщика.

А.150.3.20 Запустить PostgreSQL (база данных сборщика СМИ) и выполнить команду:

```
select s.name, sel.query from templates t inner join sources s on s.id = t.-
source_id inner join selectors sel on sel.template_id = t.id
```

А.150.3.21 Убедиться, что в результате выполнения команды отобразиться список всех шаблонов выборки данных сборщика для каждого из источников.

А.150.3.22 СПО «Амезит-В» считается выдержавшим испытания по п. А.150.3.1-А.150.3.21 программы и методики испытаний и выполняющим пункт 5.4.3.3 ТЗ на СЧ ОКР, если:

- найдены все посты, в которых употреблялись слова «Сирия» или Игил»;
- найдены все авторы, полное имя которого «Владимир»;
- отобразились все источники, в которых были сбораны публикации, с указанием количества постов по каждому источнику;
- найдены все посты, в которых обязательно употреблялись слова «Сирия» или «Аль-Нусра» и не было употреблений слова «США»;
- отобразились все объекты, в публикациях которых семантическим анализатором была найдена персона «ЭРДОГАН» (регистр не учитывался);

– отобразился писок всех пользователей подсистемы;

– отобразился список всех тематик всех пользователей;

– отобразился список всех непросмотренных уведомлений всех пользователей;

– отобразился список всех источников сборщика;

– отобразился список всех шаблонов выборки данных сборщика для каждого из источников.

А.151 Методика № 151

А.151.1 В данной методике проводится проверка СПО «Амезит-В» на соответствие требованиям пунктов 8, 8.1-8.7 ТЗ на СЧ ОКР «Амезит-В».

А.151.2 В ходе проверки оценивается состав учебно-тренировочных средств СПО «Амезит-В».

А.151.3 Проверка выполняется сравнением состава представленных эскизов учебно-тренировочных средств с утвержденным перечнем учебно-тренировочных средств. Также оценивается полнота и качество учебно-тренировочных средств в соответствии с утвержденными эскизами (исх. 120/292-9578 ФГУП «РНИИРС» от 24.10.2017 г.).

А.151.4 СПО «Амезит-В» считается выдержавшим испытания по п. А.151.3 программы и методики испытаний и выполняющим пункты 8, 8.1-8.7 ТЗ на СЧ ОКР, если:

– учебно-тренировочные средства, разработанные в СЧ ОКР, включают в свой состав:

  – учебно-технические плакаты;
  – учебно-методические материалы (наставления) по выполнению основных операций;
  – практические задания и примерные нормативы выполнения основных операций;

– учебно-методические материалы реализованы средствами современных информационных технологий (видеоролики, презентации, интерактивные видеокурсы и тренажеры и т.д.);

– состав учебно-тренировочных средств определен и согласован на этапе РКД;

– перечень и эскизы учебно-технических средств разработаны в соответствии с требованиями ГОСТ 2.605-68, согласованы с головным исполнителем в сроки, указанные в ГОСТ РВ 2.902-2005;

– состав и содержание учебно-технических средств достаточны для изучения конструкции, принципа действия, приемов использования и технического обслуживания изделия;

– проведено обучение персонала Потребителя (по согласованию) по устройству и правилам эксплуатации СПО «Амезит-В» на этапе предварительных испытаний.

А.152 Методика № 152

А.152.1 В данной методике проводится проверка СПО «Амезит-В» на соответствие требованиям пунктов 9, 9.2 ТЗ на СЧ ОКР «Амезит-В».

А.152.2 Проверяется отчет о патентных исследованиях на соответствии ГОСТ 15.011-96 «Система разработки и постановки продукции на производство. Патентные исследования. Содержание и порядок проведения».

А.152.3 Открыть отчет о патентных исследованиях и выполнить сравнение содержания отчета с требованиями ГОСТ 15.011-96 «Система разработки и постановки продукции на производство. Патентные исследования. Содержание и порядок проведения».

А.152.4 СПО «Амезит-В» считается выдержавшим испытания по п. А.152.3 программы и методики испытаний и выполняющим пункты 9, 9.2 ТЗ на СЧ ОКР, если представленный отчет о патентных исследованиях разработан в соответствие с ГОСТ 15.011-96 «Система разработки и постановки продукции на производство. Патентные исследования. Содержание и порядок проведения» содержит:

- титульный лист;
- список исполнителей;
- содержание;
- реферат;
- перечень сокращений, условных обозначений;
- общие данные об объекте исследования;
- основную часть (аналитическую);
- заключение;
- приложения:
  - задание на проведение патентных исследований;
  - регламент поиска;
  - отчет о поиске.

А.153 Методика № 153

А.153.1 В данной методике проводится проверка СПО «Амезит-В» на соответствие требованиям пунктов 9, 9.7 ТЗ на СЧ ОКР «Амезит-В».

А.153.2 Для проведения проверки необходимы аппаратные средства, входящие в состав АПК «Амезит».

А.153.3 Для проведения проверки СПО «Амезит-В» на соответствие предъявляемым требованиям необходимо выполнить действия, описанные ниже.

А.153.3.1 Выполнить запуск СПО «Амезит-В» согласно эксплуатационной документации:

- RU.ВАТС.00177-01 92 01 «Специальное программное обеспечение подсистемы формирования автономного сегмента сети передачи данных. Руководство пользователя»;
- RU.ВАТС.00178-01 92 01 «Специальное программное обеспечение подсистемы контроля сообщений автономного сегмента сети передачи данных. Руководство пользователя»;
- RU.ВАТС.00179-01 92 01 «Специальное программное обеспечение подсистемы мониторинга сети Интернет и СМИ. Руководство пользователя»;
- RU.ВАТС.00180-01 92 01 «Специальное программное обеспечение подсистемы анализа информационно-технических объектов телекоммуникационных систем. Руководство пользователя»;
- RU.ВАТС.00181-01 92 01 «Специальное программное обеспечение подсистемы первичного анализа информации. Руководство пользователя»;
- RU.ВАТС.00182-01 92 01 «Специальное программное обеспечение подсистемы ретрансляции данных с использованием промежуточных серверов. Руководство пользователя»;
- RU.ВАТС.00183-01 92 01 «Специальное программное обеспечение подсистемы подготовки, размещения и «раскрутки» специальных материалов. Руководство пользователя»;
- RU.ВАТС.00184-01 92 01 «Специальное программное обеспечение подсистемы тестирования телекоммуникационного оборудования. Руководство пользователя»;
- RU.ВАТС.00185-01 92 01 «Специальное программное обеспечение подсистемы хранения данных. Руководство пользователя»;
- RU.ВАТС.00186-01 92 01 «Специальное программное обеспечение подсистемы обработки результатов и их визуализации на интерактивном экране. Руководство пользователя».

А.153.4 Выполнить проверку СПО ПОТ в соответствии с документом RU.ВАТС.00180-01 51 01 «Специальное программное обеспечение подсистемы анализа информационно-технических объектов телекоммуникационных систем. Программа и методика испытаний».

А.153.4.1 Выполнить сканирование СПО «Амезит-В» на наличие уязвимостей посредством СПО ПОТ в соответствии с документом RU.ВАТС.00180 -01 92 01 «Специальное программное обеспечение подсистемы анализа информационно-технических объектов телекоммуникационных систем. Руководство пользователя».

А.153.4.2 Убедиться, что в ходе выполнения проверок:

- в настройках операционных систем, входящий в состав ОПО каждой подсистемы АПК «Амезит» указан адрес сервера обновлений (репозитория);
- отсутствовали сообщения об ошибках.

А.153.4.3 СПО «Амезит-В» считается выдержавшим испытания по п. А.153.3.1-А.153.4.2 программы и методики испытаний и выполняющим пункты 9, 9.7 ТЗ на СЧ ОКР, если обеспечивается соответствие защищенности ресурсов (сканирование на наличие уязвимостей) и последующее устранение обнаруженных уязвимостей.

А.154 Методика № 154

А.154.1 В данной методике проводится проверка СПО «Амезит-В» на соответствие требованиям пунктов 9, 9.8 ТЗ на СЧ ОКР «Амезит-В».

А.154.2 Для проведения проверки необходимы следующее аппаратные средства:

- АРМ оператора открытого сегмента СПО ПОР;
- АПК «Амезит».

А.154.3 Для проведения проверки СПО «Амезит-В» на соответствие предъявляемым требованиям необходимо выполнить действия, описанные ниже.

А.154.3.1 Выполнить запуск СПО «Амезит-В» согласно эксплуатационной документации:

- RU.ВАТС.00177-01 92 01 «Специальное программное обеспечение подсистемы формирования автономного сегмента сети передачи данных. Руководство пользователя»;
- RU.ВАТС.00178-01 92 01 «Специальное программное обеспечение подсистемы контроля сообщений автономного сегмента сети передачи данных. Руководство пользователя»;

– RU.ВАТС.00179-01 92 01 «Специальное программное обеспечение подсистемы мониторинга сети Интернет и СМИ. Руководство пользователя»;

– RU.ВАТС.00180-01 92 01 «Специальное программное обеспечение подсистемы анализа информационно-технических объектов телекоммуникационных систем. Руководство пользователя»;

– RU.ВАТС.00181-01 92 01 «Специальное программное обеспечение подсистемы первичного анализа информации. Руководство пользователя»;

– RU.ВАТС.00182-01 92 01 «Специальное программное обеспечение подсистемы ретрансляции данных с использованием промежуточных серверов. Руководство пользователя»;

– RU.ВАТС.00183-01 92 01 «Специальное программное обеспечение подсистемы подготовки, размещения и «раскрутки» специальных материалов. Руководство пользователя»;

– RU.ВАТС.00184-01 92 01 «Специальное программное обеспечение подсистемы тестирования телекоммуникационного оборудования. Руководство пользователя»;

– RU.ВАТС.00185-01 92 01 «Специальное программное обеспечение подсистемы хранения данных. Руководство пользователя»;

– RU.ВАТС.00186-01 92 01 «Специальное программное обеспечение подсистемы обработки результатов и их визуализации на интерактивном экране. Руководство пользователя».

А.154.3.2 Включить АРМ оператора открытого сегмента ПОР согласно документу RU.ВАТС.00186-01 34 01 «Специальное программное обеспечение подсистемы обработки результатов и их визуализации на интерактивном экране. Руководство оператора».

А.154.3.3 Включить модуль «мониторинга инфраструктуры СПО ПОР» согласно документу RU.ВАТС.00186-01 34 01 «Специальное программное обеспечение подсистемы обработки результатов и их визуализации на интерактивном экране. Руководство оператора».

А.154.3.4 Выполнить действия по отображению состояния инфраструктуры, описанные в документе RU.ВАТС.00186-01 34 01 «Специальное программное обеспечение подсистемы обработки результатов и их визуализации на интерактивном экране. Руководство оператора».

А.154.3.5 Убедиться, что в ходе выполнения проверок:

– состав и состояние узлов, отображенных в интерфейсе модуля «мониторинга инфраструктуры СПО ПОР» соответствует составу и состоянию узлов, подключенных к данному модулю по локальной вычислительно сети (ЛВС).

– отсутствовали сообщения об ошибках.

А.154.4 СПО «Амезит-В» считается выдержавшим испытания по п. А.154.3.1-А.154.3.5 программы и методики испытаний и выполняющим пункты 9, 9.8 ТЗ на СЧ ОКР, если обеспечивается инвентаризация ресурсов АПК «Амезит».

А.155 Методика № 155

А.155.1 В данной методике проводится проверка СПО «Амезит-В» на соответствие требованиям пунктов 9, 9.9 ТЗ на СЧ ОКР «Амезит-В».

А.155.2 Для проведения проверки необходимы следующее аппаратные средства:

– АРМ оператора открытого сегмента СПО ПОР;
– АПК «Амезит».

А.155.3 Для проведения проверки СПО «Амезит-В» на соответствие предъявляемым требованиям необходимо выполнить действия, описанные ниже.

А.155.3.1 Выполнить запуск СПО «Амезит-В» согласно эксплуатационной документации на СПО.

А.155.3.2 Включить АРМ оператора открытого сегмента СПО ПОР согласно документу RU.BATC.00186-01 34 01 «Специальное программное обеспечение подсистемы обработки результатов и их визуализации на интерактивном экране. Руководство оператора».

А.155.3.3 Включить модуль «модуль мониторинга инфраструктуры СПО ПОР» согласно документу RU.BATC.00186-01 34 01 «Специальное программное обеспечение подсистемы обработки результатов и их визуализации на интерактивном экране. Руководство оператора».

А.155.3.4 Выполнить действия по отображению состояния инфраструктуры, описанные в документе RU.BATC.00186-01 34 01 «Специальное программное обеспечение подсистемы обработки результатов и их визуализации на интерактивном экране. Руководство оператора».

А.155.3.5 Выполнить изменения в составе инфраструктуры АПК «Амезит»: включить или выключить АРМы или серверы, не входящие в состав модуля «мониторинга инфраструктуры СПО ПОР».

А.155.3.6 Убедиться, что при выполнении проверок:

– состав и состояние узлов, отображенных в интерфейсе модуля «мониторинга инфраструктуры СПО ПОР» изменилось при выполнении пунктов А.155.3.4 и А.155.3.5 и соответствует составу и состоянию узлов, подключенных к данному модулю по ЛВС;

– отсутствовали сообщения об ошибках.

А.155.4 СПО «Амезит-В» считается выдержавшим испытания по п. А.155.3.1-А.155.3.6 программы и методики испытаний и выполняющим пункты 9, 9.9 ТЗ на СЧ ОКР, если обеспечивается мониторинг изменений инфраструктуры АПК «Амезит».

А.156 Методика № 156

А.156.1 В данной методике проводится проверка СПО «Амезит-В» на соответствие требованиям пунктов 9, 9.10 ТЗ на СЧ ОКР «Амезит-В».

А.156.2 Для проведения проверки необходимы следующее аппаратные средства:

– АРМ администратора безопасности АПК «Амезит»;
– АПК «Амезит» (подсистем ПКС, ПРР, ПРД, ПТТ, ПМС, ПХД, ПОР).

А.156.3 Для проведения проверки СПО «Амезит-В» на соответствие предъявляемым требованиям необходимо выполнить действия, описанные ниже.

А.156.3.1 Выполнить запуск СПО «Амезит-В» согласно эксплуатационной документации:

– RU.BATC.00177-01 92 01 «Специальное программное обеспечение подсистемы формирования автономного сегмента сети передачи данных. Руководство пользователя»;
– RU.BATC.00178-01 92 01 «Специальное программное обеспечение подсистемы контроля сообщений автономного сегмента сети передачи данных. Руководство пользователя»;
– RU.BATC.00179-01 92 01 «Специальное программное обеспечение подсистемы мониторинга сети Интернет и СМИ. Руководство пользователя»;
– RU.BATC.00180-01 92 01 «Специальное программное обеспечение подсистемы анализа информационно-технических объектов телекоммуникационных систем. Руководство пользователя»;
– RU.BATC.00181-01 92 01 «Специальное программное обеспечение подсистемы первичного анализа информации. Руководство пользователя»;
– RU.BATC.00182-01 92 01 «Специальное программное обеспечение подсистемы ретрансляции данных с использованием промежуточных серверов. Руководство пользователя»;
– RU.BATC.00183-01 92 01 «Специальное программное обеспечение подсистемы подготовки, размещения и «раскрутки» специальных материалов. Руководство пользователя»;

– RU.BATC.00184-01 92 01 «Специальное программное обеспечение подсистемы тестирования телекоммуникационного оборудования. Руководство пользователя»;

– RU.BATC.00185-01 92 01 «Специальное программное обеспечение подсистемы хранения данных. Руководство пользователя»;

– RU.BATC.00186-01 92 01 «Специальное программное обеспечение подсистемы обработки результатов и их визуализации на интерактивном экране. Руководство пользователя».

А.156.3.2 Включить АРМ администратора безопасности согласно документу RU.BATC.00176-01 94 01 «Специальное программное обеспечение «Амезит-В». Руководство администратора безопасности».

А.156.3.3 Развернуть СПО «Комплекс оперативного мониторинга, реагирования и анализа данных (Комрад)» (обозначение продукта – НПЕШ.60010-02.02) на аппаратных средствах, используемых подсистемами ПКС, ПРР, ПРД, ПТТ, ПМС, ПХД, ПОР.

А.156.3.4 Выполнить действия по обеспечению сбора и анализа событий информационной безопасности, поступающих с контролируемых подсистем АПК «Амезит», описанных в документе RU.BATC.00176-01 94 01 «Специальное программное обеспечение «Амезит-В». Руководство администратора безопасности».

А.156.3.5 Убедиться, что в ходе выполнения проверок:

– СПО «Комплекс оперативного мониторинга, реагирования и анализа данных (Комрад)» (обозначение продукта – НПЕШ.60010-02.02) развернут согласно эксплуатационной документации продукта;

– отсутствовали сообщения об ошибках.

А.156.4 СПО «Амезит-В» считается выдержавшим испытания по п. А.156.3.1-А.156.3.5 программы и методики испытаний и выполняющим пункты 9, 9.10 ТЗ на СЧ ОКР, если обеспечивается сбор и анализ событий информационной безопасности, поступающих с контролируемых подсистем АПК «Амезит».

А.157 Методика № 157

А.157.1 В данной методике проводится проверка СПО «Амезит-В» на соответствие требованиям пунктов 9, 9.11 ТЗ на СЧ ОКР «Амезит-В».

А.157.2 Для проведения проверки необходимы следующее аппаратные средства:

– АРМ администратора безопасности;

– АПК «Амезит».

А.157.3 Для проведения проверки СПО «Амезит-В» на соответствие предъявляемым требованиям необходимо выполнить действия, описанные ниже.

А.157.3.1 Выполнить запуск СПО «Амезит-В» согласно эксплуатационной документации на СПО.

А.157.3.2 Включить АРМ администратора безопасности согласно документу RU.ВАТС.00176-01 94 01 «Специальное программное обеспечение «Амезит-В». Руководство администратора безопасности».

А.157.3.3 Развернуть СПО «Комплекс оперативного мониторинга, реагирования и анализа данных (Комрад)» (обозначение продукта – НПЕШ.60010-02.02) на аппаратных средствах, используемых подсистемами ПКС, ПРР, ПРД, ПТТ, ПМС, ПХД, ПОР.

А.157.3.4 Выполнить действия по обеспечению визуализации полученных данных и оповещения администратора безопасности об инцидентах информационной безопасности, описанных в документе RU.ВАТС.00176-01 94 01 «Специальное программное обеспечение «Амезит-В». Руководство администратора безопасности».

А.157.3.5 Убедиться, что в ходе выполнения проверок:

- СПО «Комплекс оперативного мониторинга, реагирования и анализа данных (Комрад)» (обозначение продукта – НПЕШ.60010-02.02) развернут согласно эксплуатационной документации продукта;
- отсутствовали сообщения об ошибках.

А.157.4 СПО «Амезит-В» считается выдержавшим испытания по п. А.157.3.1-А.157.3.5 программы и методики испытаний и выполняющим пункты 9, 9.11 ТЗ на СЧ ОКР, если обеспечивается визуализация полученных данных и оповещение администратора безопасности об инцидентах информационной безопасности.

А.158 Методика № 158

А.158.1 В данной методике проводится проверка СПО «Амезит-В» на соответствие требованиям пунктов 9, 9.13 ТЗ на СЧ ОКР «Амезит-В».

А.158.2 Проверка выполняется путем визуального просмотра исходного кода СПО.

А.158.3 СПО «Амезит-В» считается выдержавшим испытания по п. А.158.2 программы и методики испытаний и выполняющим пункты 9, 9.13 ТЗ на СЧ ОКР, если:

- в скриптах и конфигурационных файлах данных СПО «Амезит-В» отсутствуют любые комментарии;

– наименования модулей, классов, генерируемые данные и т.п. не раскрывают национальную принадлежность, сведения о разработчике и Заказчике.

А.159 Методика № 159

А.159.1 В данной методике проводится проверка СПО «Амезит-В» на соответствие требованиям пунктов 9, 9.15 ТЗ на СЧ ОКР «Амезит-В».

А.159.2 Для проведения проверки необходимы аппаратные средства, из состава АПК «Амезит».

А.159.3 Для проведения проверки СПО «Амезит-В» на соответствие предъявляемым требованиям необходимо выполнить действия, описанные ниже.

А.159.3.1 Выполнить запуск СПО «Амезит-В» согласно эксплуатационной документации:

– RU.ВАТС.00177-01 92 01 «Специальное программное обеспечение подсистемы формирования автономного сегмента сети передачи данных. Руководство пользователя»;

– RU.ВАТС.00178-01 92 01 «Специальное программное обеспечение подсистемы контроля сообщений автономного сегмента сети передачи данных. Руководство пользователя»;

– RU.ВАТС.00179-01 92 01 «Специальное программное обеспечение подсистемы мониторинга сети Интернет и СМИ. Руководство пользователя»;

– RU.ВАТС.00180-01 92 01 «Специальное программное обеспечение подсистемы анализа информационно-технических объектов телекоммуникационных систем. Руководство пользователя»;

– RU.ВАТС.00181-01 92 01 «Специальное программное обеспечение подсистемы первичного анализа информации. Руководство пользователя»;

– RU.ВАТС.00182-01 92 01 «Специальное программное обеспечение подсистемы ретрансляции данных с использованием промежуточных серверов. Руководство пользователя»;

– RU.ВАТС.00183-01 92 01 «Специальное программное обеспечение подсистемы подготовки, размещения и «раскрутки» специальных материалов. Руководство пользователя»;

– RU.ВАТС.00184-01 92 01 «Специальное программное обеспечение подсистемы тестирования телекоммуникационного оборудования. Руководство пользователя»;

– RU.ВАТС.00185-01 92 01 «Специальное программное обеспечение подсистемы хранения данных. Руководство пользователя»;

– RU.ВАТС.00186-01 92 01 «Специальное программное обеспечение подсистемы обработки результатов и их визуализации на интерактивном экране. Руководство пользователя».

А.159.3.2 Выполнить испытания СПО ППА согласно документу RU.ВАТС.00181-01 51 01 «Специальное программное обеспечение подсистемы первичного анализа информации. Программа и методика испытаний».

А.159.3.3 Выполнить настройку модуля «мониторинга инфраструктуры СПО ПОР» согласно документу RU.ВАТС.00181-01 32 01 «Специальное программное обеспечение подсистемы первичного анализа информации. Руководство системного программиста».

А.159.3.4 Подключить устройство «Скат анализатор трафика», входящее в состав ППА, к каналу передачи данных. Подключение выполнить в соответствии с документом RU.ВАТС.00181-01 34 01 «Специальное программное обеспечение подсистемы первичного анализа информации. Руководство оператора».

А.159.3.5 Выполнить анализ передаваемого в канале трафика в соответствии с документом RU.ВАТС.00181-01 92 01 «Специальное программное обеспечение подсистемы первичного анализа информации. Руководство пользователя».

А.159.3.6 Повторить анализ для каждого канала передачи данных.

А.159.3.7 Убедиться, что в ходе выполнения проверок:

– в результате анализа СПО ППА не выдало сообщений об аномальности трафика и возможности компрометации протоколов;
– при выполнении вышеуказанных действий данной методики отсутствовали сообщения об ошибках.

А.159.4 СПО «Амезит-В» считается выдержавшим испытания по п. А.159.3.1-А.159.3.7 программы и методики испытаний и выполняющим пункты 9, 9.15 ТЗ на СЧ ОКР, если СПО «Амезит-В» передает данные о своем текущем состоянии с использованием устойчивых к обнаружению и компрометации протоколов.

А.160 Методика № 160

А.160.1 В данной методике проводится проверка СПО «Амезит-В» на соответствие требованиям пунктов 9, 9.16 ТЗ на СЧ ОКР «Амезит-В».

А.160.2 Для проведения проверки необходимы следующее аппаратные средства: АПК «Амезит».

А.160.3 Для проведения проверки СПО «Амезит-В» на соответствие предъявляемым требованиям необходимо выполнить действия, описанные ниже.

А.160.3.1 Выполнить запуск СПО «Амезит-В» согласно эксплуатационной документации:

- RU.BATC.00177-01 92 01 «Специальное программное обеспечение подсистемы формирования автономного сегмента сети передачи данных. Руководство пользователя»;
- RU.BATC.00178-01 92 01 «Специальное программное обеспечение подсистемы контроля сообщений автономного сегмента сети передачи данных. Руководство пользователя»;
- RU.BATC.00179-01 92 01 «Специальное программное обеспечение подсистемы мониторинга сети Интернет и СМИ. Руководство пользователя»;
- RU.BATC.00180-01 92 01 «Специальное программное обеспечение подсистемы анализа информационно-технических объектов телекоммуникационных систем. Руководство пользователя»;
- RU.BATC.00181-01 92 01 «Специальное программное обеспечение подсистемы первичного анализа информации. Руководство пользователя»;
- RU.BATC.00182-01 92 01 «Специальное программное обеспечение подсистемы ретрансляции данных с использованием промежуточных серверов. Руководство пользователя»;
- RU.BATC.00183-01 92 01 «Специальное программное обеспечение подсистемы подготовки, размещения и «раскрутки» специальных материалов. Руководство пользователя»;
- RU.BATC.00184-01 92 01 «Специальное программное обеспечение подсистемы тестирования телекоммуникационного оборудования. Руководство пользователя»;
- RU.BATC.00185-01 92 01 «Специальное программное обеспечение подсистемы хранения данных. Руководство пользователя»;
- RU.BATC.00186-01 92 01 «Специальное программное обеспечение подсистемы обработки результатов и их визуализации на интерактивном экране. Руководство пользователя».

А.160.3.2 Выполнить испытания СПО ППА согласно документу RU.BATC.00181-01 51 01 «Специальное программное обеспечение подсистемы первичного анализа информации. Программа и методика испытаний».

А.160.3.3 Выполнить настройку модуля «мониторинга инфраструктуры СПО ПОР» согласно документу RU.BATC.00186-01 32 01 «Специальное

программное обеспечение подсистемы обработки результатов и их визуализации на интерактивном экране. Руководство системного программиста».

А.160.3.4 Подключить устройство «Скат анализатор трафика», входящее в состав подсистемы ППА к каналу передачи данных в соответствии с документом RU.BATC.00186-01 34 01 «Специальное программное обеспечение подсистемы обработки результатов и их визуализации на интерактивном экране. Руководство оператора».

А.160.3.5 Выполнить MiTM атаку на канал передачи данных согласно документу RU.BATC.00186-01 92 01 «Специальное программное обеспечение подсистемы обработки результатов и их визуализации на интерактивном экране. Руководство пользователя».

А.160.3.6 Повторить анализ для каждого канала передачи данных.

А.160.3.7 Убедиться, что в ходе выполнения проверок:

- ни одна из MiTM атак, совершенных СПО ППА, не была успешной;
- отсутствовали сообщения об ошибках.

А.160.4 СПО «Амезит-В» считается выдержавшим испытания по п. А.160.3.1-А.160.3.7 программы и методики испытаний и выполняющим пункты 9, 9.16 ТЗ на СЧ ОКР, если СПО «Амезит-В» при организации информационного обмена обеспечивает защиту от MiTM атак.

А.161 Методика № 161

А.161.1 В данной методике проводится проверка СПО «Амезит-В» на соответствие требованиям пунктов 9, 9.17 ТЗ на СЧ ОКР «Амезит-В».

А.161.2 Для проведения проверки необходимы аппаратные средства, входящие в АПК «Амезит».

А.161.3 Для проведения проверки СПО «Амезит-В» на соответствие предъявляемым требованиям необходимо выполнить действия, описанные ниже.

А.161.3.1 Выполнить запуск СПО «Амезит-В» согласно эксплуатационной документации:

- RU.BATC.00177-01 92 01 «Специальное программное обеспечение подсистемы формирования автономного сегмента сети передачи данных. Руководство пользователя»;
- RU.BATC.00178-01 92 01 «Специальное программное обеспечение подсистемы контроля сообщений автономного сегмента сети передачи данных. Руководство пользователя»;

– RU.BATC.00179-01 92 01 «Специальное программное обеспечение подсистемы мониторинга сети Интернет и СМИ. Руководство пользователя»;

– RU.BATC.00180-01 92 01 «Специальное программное обеспечение подсистемы анализа информационно-технических объектов телекоммуникационных систем. Руководство пользователя»;

– RU.BATC.00181-01 92 01 «Специальное программное обеспечение подсистемы первичного анализа информации. Руководство пользователя»;

– RU.BATC.00182-01 92 01 «Специальное программное обеспечение подсистемы ретрансляции данных с использованием промежуточных серверов. Руководство пользователя»;

– RU.BATC.00183-01 92 01 «Специальное программное обеспечение подсистемы подготовки, размещения и «раскрутки» специальных материалов. Руководство пользователя»;

– RU.BATC.00184-01 92 01 «Специальное программное обеспечение подсистемы тестирования телекоммуникационного оборудования. Руководство пользователя»;

– RU.BATC.00185-01 92 01 «Специальное программное обеспечение подсистемы хранения данных. Руководство пользователя»;

– RU.BATC.00186-01 92 01 «Специальное программное обеспечение подсистемы обработки результатов и их визуализации на интерактивном экране. Руководство пользователя».

А.161.3.2 Для СПО каждой подсистемы:

– выполнить действия, регистрируемые в журнале событий СПО, в соответствии с руководством оператора каждого СПО;

– открыть журнал событий.

А.161.3.3 Убедиться, что в ходе выполнения проверок:

– регистрируемые действия операторов были отображены в журнале событий каждой подсистемы;

– отсутствовали сообщения об ошибках.

А.161.4 СПО «Амезит-В» считается выдержавшим испытания по п. А.161.3.1-А.161.3.3 программы и методики испытаний и выполняющим пункты 9, 9.17 ТЗ на СЧ ОКР, если все действия операторов регистрируются и записываются в хранилищах информации для обеспечения проведения полноценного анализа порядка действий должностных лиц.

А.162 Методика № 162

А.162.1 В данной методике проводится проверка СПО «Амезит-В» на соответствие требованиям пунктов 9, 9.18 ТЗ на СЧ ОКР «Амезит-В».

А.162.2 Для проведения проверки необходимы аппаратные средства, входящие в состав АПК «Амезит».

А.162.3 Для проведения проверки СПО «Амезит-В» на соответствие предъявляемым требованиям необходимо выполнить действия, описанные ниже.

А.162.3.1 Выполнить запуск СПО «Амезит-В» согласно эксплуатационной документации:

- RU.BATC.00177-01 92 01 «Специальное программное обеспечение подсистемы формирования автономного сегмента сети передачи данных. Руководство пользователя»;
- RU.BATC.00178-01 92 01 «Специальное программное обеспечение подсистемы контроля сообщений автономного сегмента сети передачи данных. Руководство пользователя»;
- RU.BATC.00179-01 92 01 «Специальное программное обеспечение подсистемы мониторинга сети Интернет и СМИ. Руководство пользователя»;
- RU.BATC.00180-01 92 01 «Специальное программное обеспечение подсистемы анализа информационно-технических объектов телекоммуникационных систем. Руководство пользователя»;
- RU.BATC.00181-01 92 01 «Специальное программное обеспечение подсистемы первичного анализа информации. Руководство пользователя»;
- RU.BATC.00182-01 92 01 «Специальное программное обеспечение подсистемы ретрансляции данных с использованием промежуточных серверов. Руководство пользователя»;
- RU.BATC.00183-01 92 01 «Специальное программное обеспечение подсистемы подготовки, размещения и «раскрутки» специальных материалов. Руководство пользователя»;
- RU.BATC.00184-01 92 01 «Специальное программное обеспечение подсистемы тестирования телекоммуникационного оборудования. Руководство пользователя»;
- RU.BATC.00185-01 92 01 «Специальное программное обеспечение подсистемы хранения данных. Руководство пользователя»;
- RU.BATC.00186-01 92 01 «Специальное программное обеспечение подсистемы обработки результатов и их визуализации на интерактивном экране. Руководство пользователя».

А.162.3.2 Открыть АРМ оператора СПО подсистем ПКС, ПМС, ПХД, ПТТ, ПРР, ПРД.

А.162.3.3 Выполнить вход на произвольный адрес в сети Интернет.

А.162.3.4 Повторить анализ для каждого канала передачи данных.

А.162.3.5 Убедиться, что в ходе выполнения проверок:

- было заблокировано выполнение входа на произвольный адрес в сети Интернет с рабочих мест СПО подсистем ПКС, ПМС, ПХД, ПТТ;
- выполнение входа на произвольный адрес в сети Интернет с рабочих мест СПО подсистем ПРР и ПРД было прервано сообщением об опасности совершаемых действий;
- отсутствовали сообщения об ошибках.

А.162.3.6 СПО «Амезит-В» считается выдержавшим испытания по п. А.162.3.1-А.162.3.5 программы и методики испытаний и выполняющим пункты 9, 9.18 ТЗ на СЧ ОКР, если СПО «Амезит-В» исключает возможность использование функциональных возможностей комплекса оператором в личных целях.

А.163 Методика № 163

А.163.1 В данной методике проводится проверка СПО «Амезит-В» на соответствие требованиям пунктов 13.1-13.5.1, 13.7-13.10, 13.14-13.16 ТЗ на СЧ ОКР «Амезит-В».

А.163.2 В ходе проверки оценивается порядок выполнения и приемки этапов СПО «Амезит-В».

А.163.3 Проверка выполнения анализом представленной отчетной документации.

А.163.4 СПО «Амезит-В» считается выдержавшим испытания по п. А.163.3 программы и методики испытаний и выполняющим пункты 13.1-13.5.1, 13.7-13.10, 13.14-13.16 ТЗ на СЧ ОКР, если:

- порядок выполнения и приемки этапов СЧ ОКР осуществлялся в соответствии с ГОСТ РВ 15.203-2001;
- представлены уведомления о готовности этапов к приемке;
- вместе с уведомлением для организации приемки этапов представлены:
- документы, предусмотренные п. 5.2.11 ГОСТ РВ 15.203-2001;
- отчетная научно-техническая документация, предусмотренная ТЗ на СЧ ОКР;
- учетные данные о результатах, полученных в ОКР, по форме № 1, утвержденной приказом Минюста России, Минпромнауки России от 17 июля 2003 г. № 173/178 (зарегистрирован в Минюсте России от 29 июля 2003 г. № 4933) на бумажном носителе в одном экземпляре.

Приложение Б

Общая схема подключения аппаратных средств СПО «Амезит-В»

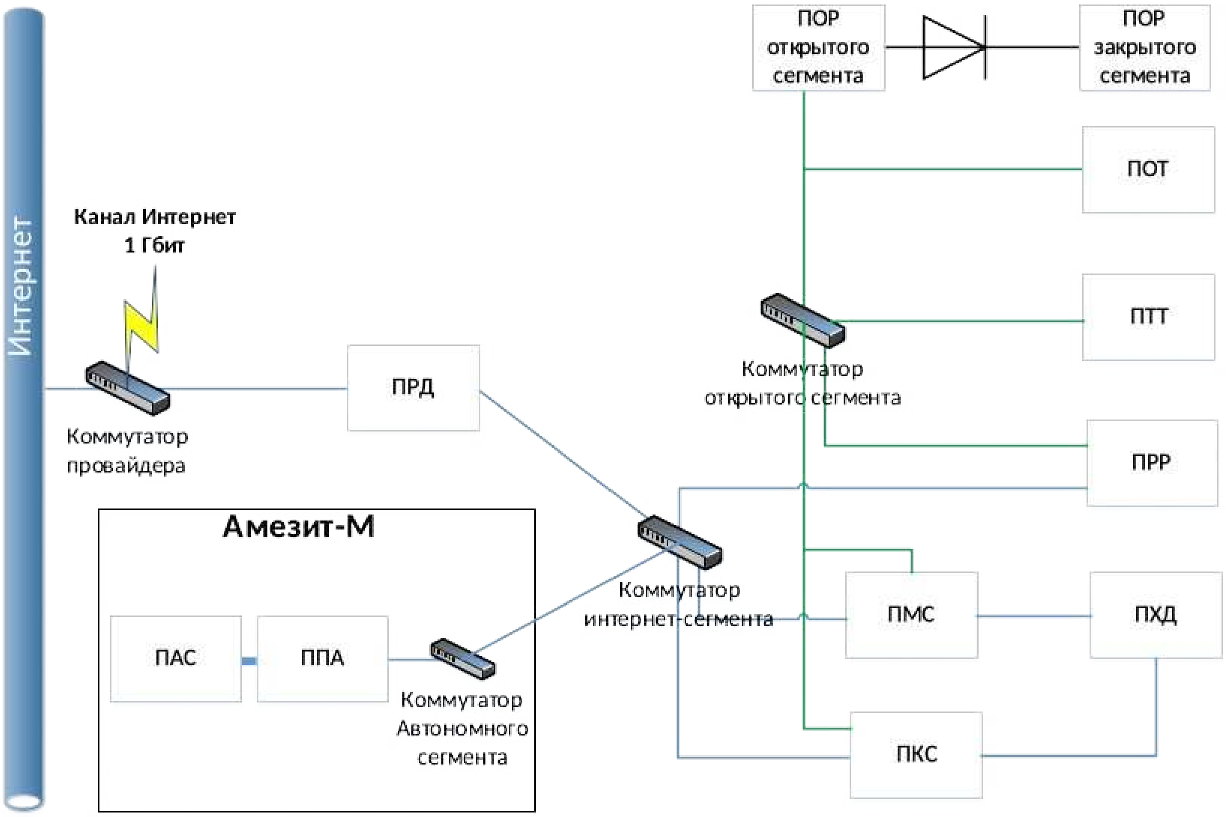


Рисунок 1 – Общая схема подключения

Схемы подключения аппаратных средств СПО ПОТ, ПАС, ППА, ПКС

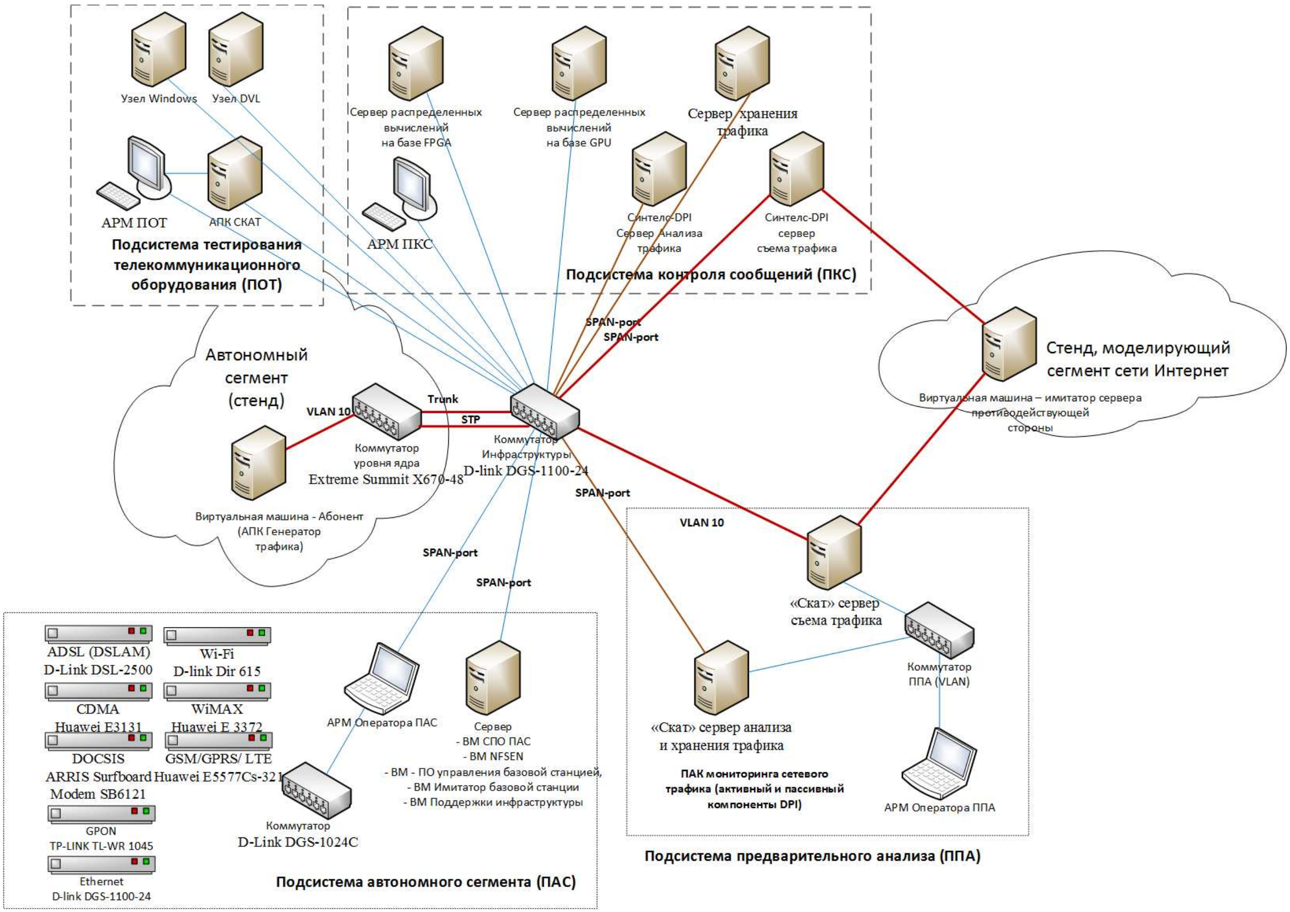


Рисунок 2 – Схема испытательного стенда СПО ПОТ

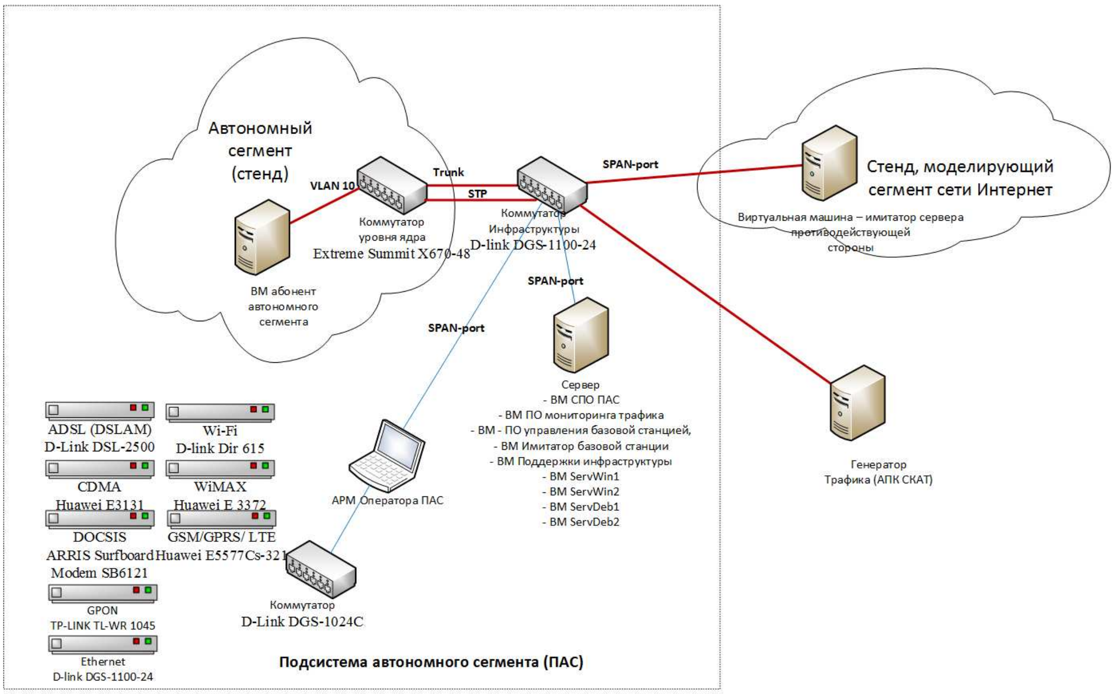


Рисунок 3 – Схема испытательного стенда СПО ПАС

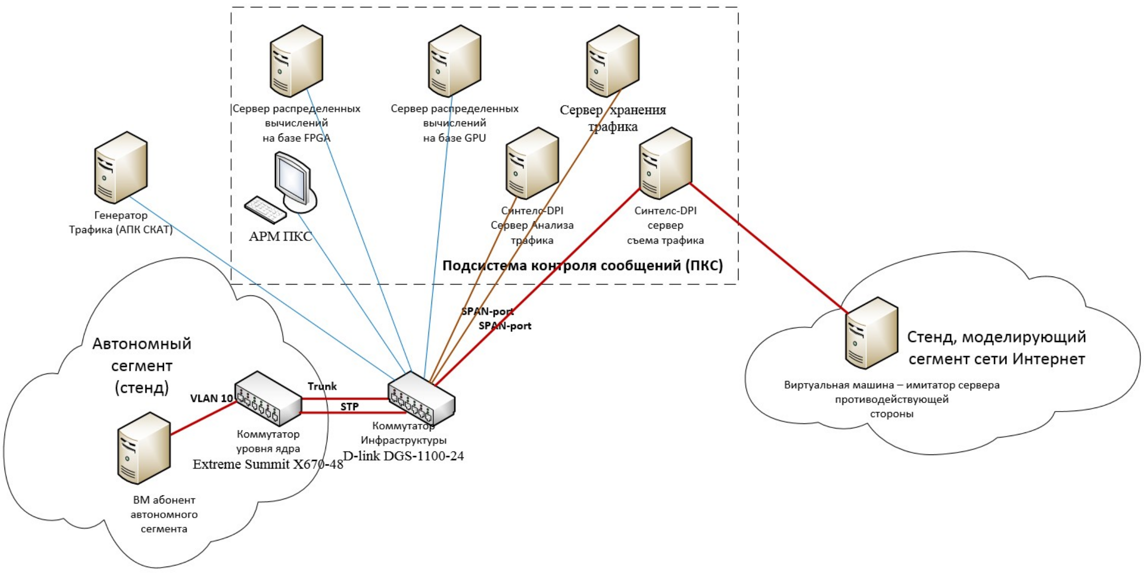


Рисунок 4 – Схема испытательного стенда СПО ПКС

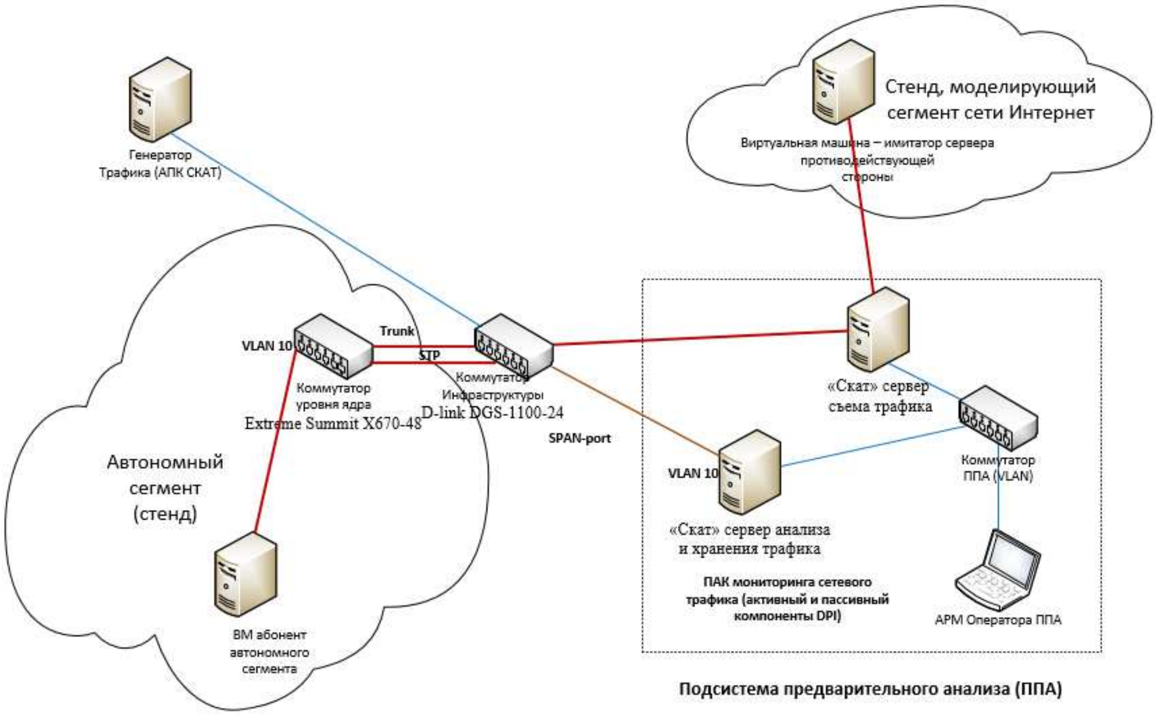


Рисунок 5 – Схема испытательного стенда СПО ППА

Состав испытательного стенда СПО ПОТ приведен в таблице ниже.

№	Название	Назначение	ОС	Сервисы и утилиты	IP-адрес	Аутентификационная информация
1	АРМ ПОТ	АРМ оператора ПОТ	Kali Linux 2.0 (2018.1) x64	Сканер уязвимостей ПОТ, ssh, генератор трафика АСУТП trafficGenerator	10.0.6.57	ssh{root:O9052p}
2	АПК СКАТ	Эмулятор АПК СКАТ «Генератор трафика»	CentOS 6 x64	ftp, ssh, apache 2, php	10.0.6.167	ssh{root:Kn2018eeDeep} ftp{ftpu:PassWd6231}
3	DD-WRT	Эмулятор коммутационного оборудования (сервисов администрирования)	CentOS 6 x32	ssh, apache 2, dhcp сервер	10.0.6.207	http{admin:admin} ssh{root:ad-min}
4	Bruteforce	Эмулятор	CentOS	ssh, bfd	10.0.6.31	ssh{root:Gw

	detector	системы обнаружения вторжений (система детектирования попыток перебора паролей к сервисам администрирования)	7 x64			1547!}
5	АСУТП Сервер	Эмулятор компонентов АСУТП	Windows 7 x32	WinCC	10.0.6.168	rdp{admin:AsutP}
6	АСУТП Клиент	Эмулятор АРМ оператора АСУТП	Windows 10 x32	Симулятор процессов АСУТП, step7, OPC	10.0.6.215	rdp{admin:AsutP}
7	GNS	Эмулятор сетевой инфраструктуры	Debian 8 x64	ssh, gns	10.0.6.204	ssh{root:Gw1547}
8	DVL	Эмулятор узла Linux с набором уязвимостей (Damn Vulnerable Linux)	DVL 1.5 x64	ssh	10.0.6.148	ssh{root:toor}

Схема подключения аппаратных средств СПО ПРД

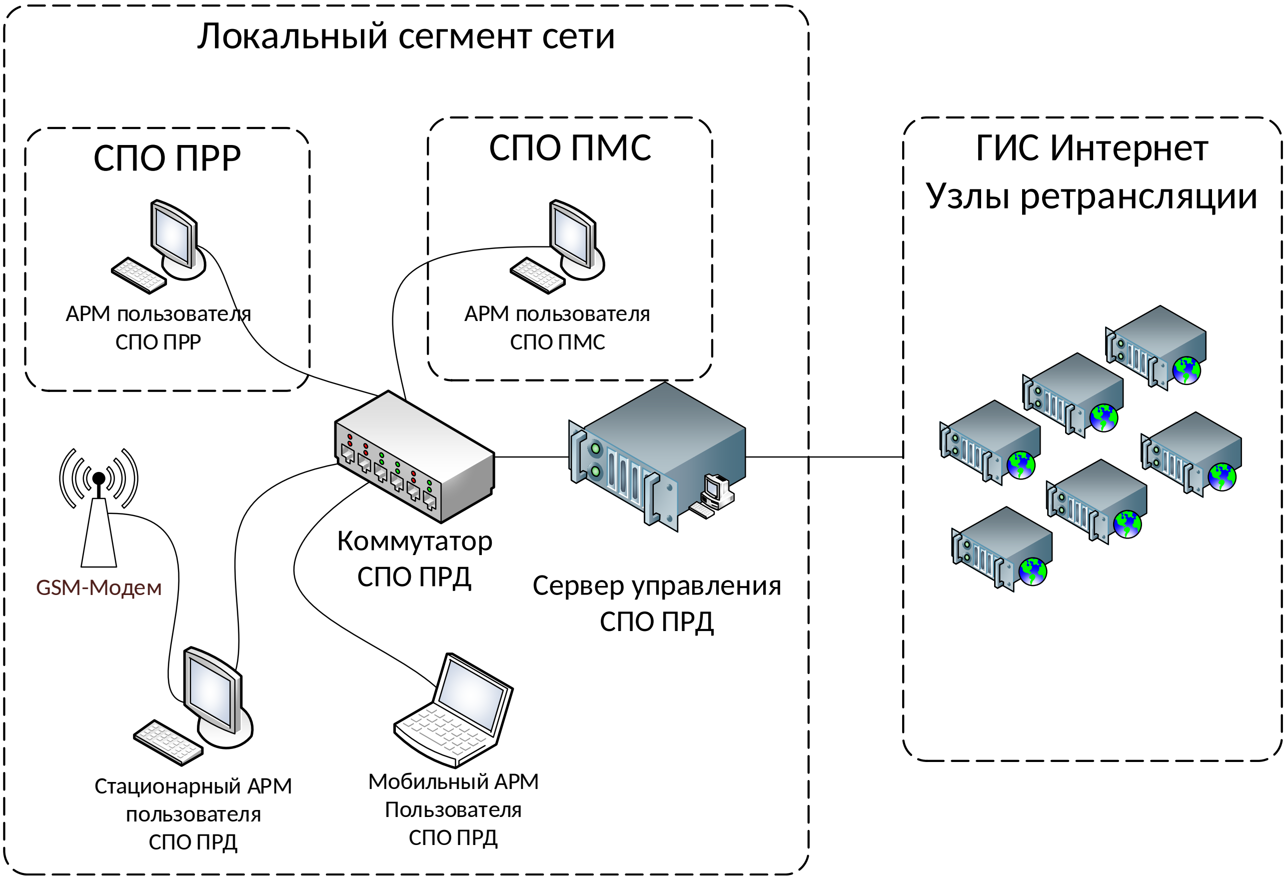


Рисунок 6 – Схема испытательного стенда СПО ПРД

Приложение Е

Список сокращений

АПК	Аппаратно-программный комплекс
ИБ	Информационная безопасность
НСД	Несанкционированный доступ
ОЗУ	Оперативное запоминающее устройство
ОКР	Опытно-конструкторская работа
ОС	Операционная система
ПАС	Подсистема формирования автономного сегмента сети передачи данных
ПКС	Подсистема контроля сообщений автономного сегмента
ПМС	Подсистема мониторинга сети Интернет и СМИ
ПО	Программное обеспечение
ПОР	Подсистема обработки результатов
ПОТ	Подсистема анализа информационно-технических объектов телекоммуникационных систем
ППА	Подсистема первичного анализа трафика автономного сегмента
ПРД	Подсистема ретрансляции данных с использованием промежуточных серверов
ПРР	Подсистема подготовки, размещения и раскрутки специальных материалов
ПСС	Проводная сеть связи
ПТТ	Подсистема тестирования телекоммуникационного оборудования
ПХД	Подсистема хранения данных
СМИ	Средства массовой информации
СПО	Специальное программное обеспечение
СЧ	Составная часть
СЧ ОКР	Составная часть опытно-конструкторской работы
ТЗ	Техническое задание

Лист согласования

от Заказчика: от Исполнителя: